Załącznik nr 2 do SWZ **SPZOZ/PN/09/2022**

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

MODERNIZACJA I ROZWÓJ E-USŁUG W RAMACH PODKARPACKIEGO SYSTEMU INFORMACJI MEDYCZNEJ (PSIM) W SAMODZIELNYM PUBLICZNYM ZAKŁADZIE OPIEKI ZDROWOTNEJ W SANOKU

SANOK 2022

Rozdział I
Założenia początkowe i wymagania ogólne

1. Cel projektu

Celem projektu „Modernizacja i rozwój e-usług w ramach Podkarpackiego Systemu Informacji Medycznej (PSIM) w SPZOZ w Sanoku" jest podniesienie poziomu jakości oraz zwiększenie efektywności i dostępności usług w sektorze ochrony zdrowia na terenie województwa podkarpackiego.

Zakres przedmiotowy projektu zapewni skuteczne narzędzia dostępu obywateli do informacji sektora publicznego w obszarze ochrony zdrowia oraz umożliwi im komunikowanie się przy wykorzystaniu systemów teleinformatycznych. Modernizacja i rozszerzenie e-usług publicznych podniesie efektywność działania jednostek sektora ochrony zdrowia z terenu województwa podkarpackiego.

W ramach działań zaplanowanych przez Wnioskodawcę w odniesieniu do e-usług (e-Informacja, e-Rejestracja, Elektroniczny Rekord Pacjenta, Regionalne Repozytorium EDM) wymagana jest modernizacja oraz aktualizacja posiadanych przez niego zasobów informatycznych. Skrócony opis e-Usług realizowanych w ramach modernizacji projektu dostępny jest pod adresem: *https://www.rpo.podkarpackie.pl/images/dok/OS_II_VI/2019/nab_2_1_004/zm/RK_11_3_Skrocony_opis_e-uslug_w_ramach_modernizacji_PSIM_oraz_karta_integracji_z_RCIM_po_modernizacji.pdf*.

Projekt zakłada, że wszystkie utrzymywane e-usługi muszą być dostosowane do wymogów prawa w szczególności w zakresie zgodności z wytycznymi Centrum e-Zdrowie (CeZ, dotychczas CSIOZ) oraz Ministerstwa Zdrowia. Modyfikowany Szpitalny System Informatyczny (SSI) musi zapewnić integrację funkcjonalną z systemem teleinformatycznym, o którym mowa w zapisach ustawy o systemie informacji w ochronie zdrowia (tj. Dz.U. z 2017 roku, poz. 1845 z poźn. zm.), co najmniej w zakresie opisanym w dokumentach: „Opis usług biznesowych Systemu P1 wykorzystywanych w systemach usługodawców", „Opis funkcjonalny Systemu P1 z perspektywy integracji systemów zewnętrznych" opublikowanych przez Centrum e-Zdrowie oraz „Minimalne wymagania dla systemów usługodawców (*https://www.gov.pl/web/zdrowie/minimalne-wymagania-dla-systemow-uslugodawcow*) oraz dokumentacja integracyjna dla obszaru Zdarzeń Medycznych i Indeksów EDM.
W zakresie integracji i komplementarności z centralnymi systemami e-zdrowia, na Wykonawcy będzie spoczywał obowiązek dostosowania zaoferowanego rozwiązania do wymagań ujętych w dokumentach publikowanych poprzez Centrum e-Zdrowie, w tym w szczególności do:

- zakresu funkcjonalnego Projektu P1,
- opisu funkcjonalnego Systemu P1 z perspektywy integracji systemów zewnętrznych.

Dokumenty te dostępne są na stronie internetowej Centrum e-Zdrowie, pod adresem: *http://ezdrowie.gov.pl*.

System P1 dostępny będzie dla odpowiednio zarejestrowanych w Centrum e-Zdrowie systemów usługodawców i systemów regionalnych wyłącznie poprzez standardowe interfejsy Web Services. Wymagane jest dwustronne uwierzytelnianie systemów nawiązujących komunikację, a także podpisywanie komunikatów certyfikatem dostarczanym bądź wskazanym przez Centrum e-Zdrowie.
W przypadku informacji o zdarzeniu medycznym – obowiązuje Model Informacji o Zdarzeniu Medycznym i Indeksie Dokumentacji Medycznej (dalej: EDMiZM) publikowany przez Centrum e-Zdrowie.

W przypadku rejestru (indeksu) Elektronicznej Dokumentacji Medycznej – obowiązuje EDMiZM publikowany przez Centrum e-Zdrowie.
Zgoda pacjenta na udostępnienie jego dokumentacji medycznej – funkcjonalność ta jest wymagana i powinna być zgodna z modelem dokumentu zgody oraz modelami interfejsów pozwalających na wnioskowanie o zgodę, które zostaną opublikowane przez Centrum e-Zdrowie.
Wymiana Elektronicznej Dokumentacji Medycznej (dalej: EDM) – funkcjonalność ta jest wymagana i powinna być zgodna z modelem wniosku i dokumentu udostępnienia oraz modelami interfejsów, które zostaną opublikowane przez Centrum e-Zdrowie.
Jednocześnie, zaoferowane elementy i rozwiązania powinny spełniać następujące założenia funkcjonalne:

- Prowadzenie i wymiana Elektronicznej Dokumentacji Medycznej (EDM), w tym indywidualnej dokumentacji medycznej (wewnętrznej i zewnętrznej), uwzględniać musi rozwiązania umożliwiające zbieranie przez podmiot udzielający świadczeń opieki zdrowotnej jednostkowych danych medycznych w elektronicznym rekordzie pacjenta oraz tworzenie EDM zgodnej co najmniej ze standardem HL7 CDA, opracowanym i opublikowanym przez Centrum e-Zdrowie – Polską Implementacją Krajową HL7 CDA (tzw. IG).
- Szpitalny System Informatyczny powinien uwzględniać funkcjonalności dotyczące prowadzenia repozytorium EDM (z obsługą przechowywania EDM) oraz uwzględniać rozwiązania zapewniające wymianę EDM pomiędzy repozytorium Zamawiającego, a Platformą P1. Platforma P1 będzie zawierała katalog EDM, w którym znajdować się będą informacje o EDM tworzonym i przechowywanym u Zamawiającego.
- Repozytorium EDM powinno realizować, co najmniej usługę przyjmowania, archiwizacji i udostępniania EDM zgodnej z HL7 CDA, a w przypadku repozytoriów badań obrazowych, przyjmowania, archiwizacji i udostępniania obiektów DICOM.

Cel projektu zostanie osiągnięty poprzez zakup i instalację sprzętu informatycznego i niezbędnego oprogramowania, oraz wdrożenie warstwy narzędziowej umożliwiającej osiągnięcie wyższej jakości usług publicznych świadczonych drogą elektroniczną w zakresie komunikacji wszystkich uczestników Podkarpackiego Systemu Informacji Medycznej na terenie województwa podkarpackiego, do czego niezbędnym jest również utrzymanie integracji z platformą regionalną RCIM po jej modernizacji.

Dodatkową korzyścią realizacji projektu jest zapewnienie ciągłej dostępności krytycznych aplikacji i danych oraz zapewnienie elastyczności i skalowalności rozwiązania. Osiągnięte to zostanie poprzez:

- wdrożenie środowiska macierzowego wysokiej dostępności (HA),
- wirtualizację środowiska serwerowego,
- zwiększenie przepustowości szkieletu sieci do 10G,
- modernizację środowiska backupu i archiwizacji danych,
- modernizację systemu bezpieczeństwa (HA),
- modernizację wyposażenia serwerowni,
- eliminację pojedynczego punktu awarii (zastosowanie redundancji rozwiązań systemów i infrastruktury serwerowej).

Poniżej przedstawiono szczegółowe zasady instalacji, serwisu oraz opis parametrów technicznych wymaganych dostaw.

2. Wymagania ogólne dla urządzeń i oprogramowania

- Wykonawca będzie zobowiązany do nieodpłatnego usuwania Wad Przedmiotu zamówienia rozumianych jako Awaria lub Usterka zgodnie z definicjami jak poniżej:
  - Awaria – Kategoria Wady w infrastrukturze sprzętowej lub programowej powodującej brak działania lub niepoprawne działanie Przedmiotu Zamówienia u Zamawiającego, uniemożliwiające jego użytkowanie. Sytuacja, w której urządzenie w ogóle nie funkcjonuje lub nie jest możliwe realizowanie istotnych funkcjonalności Komponentów/Produktów Przedmiotu Zamówienia,
  - Usterka – Należy przez to rozumieć kategorię Wady w infrastrukturze sprzętowej lub programowej oznaczającą funkcjonowanie niezgodne z opisem Dokumentacji oraz SOPZ, nie wpływającą istotnie na funkcjonowanie dostarczanego rozwiązania u Zamawiającego.
- Przedmiot zamówienia musi być dostarczany, wdrożony i zainstalowany w całości w siedzibie Zamawiającego, w wyznaczonych przez niego lokalizacjach i punktach (w sposób umożliwiający ich prawidłową wentylację).
- Szczegóły dotyczące instalacji i uruchomienia sprzętu zostaną ustalone w trakcie Analizy Przedwdrożeniowej (dotyczy pakietów / zadań 4, 5 i 6).
- Produkt jest to elementarny efekt działań/prac/dostaw objętych całym zakresem Przedmiotu Zamówienia wykonywanych przez Wykonawcę podczas realizacji Umowy w poszczególnych Etapach.
- Oprogramowanie musi zostać skonfigurowane tak, aby działało poprawnie zgodnie z jego przeznaczeniem i architekturą systemu oraz zapewniało prawidłową pracę oprogramowania aplikacyjnego.
- Oprogramowanie aplikacyjne musi zostać zainstalowane przez Wykonawcę w szczególności z wykorzystaniem sprzętu dostarczanego przez Wykonawcę i w środowiskach informatycznych Zamawiającego.
- Komponenty (rozumiane jako integralna część dostawy i wdrożenia Przedmiotu Zamówienia, składające się przynajmniej z jednego Produktu lub wielu Produktów powiązanych ze sobą merytorycznie) podlegają usługom projektowania, dostaw, instalacji, konfiguracji i wdrożenia.
- Wykonawca musi posiadać prawo do sprzedaży oferowanego oprogramowania oraz autoryzację dotyczącą jego wdrażania i serwisowania.
- Całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów.
- Dostarczone rozwiązania teleinformatyczne, ze szczególnym uwzględnieniem dostarczanego i wdrażanego Oprogramowania, muszą być zgodne z powszechnie obowiązującymi przepisami prawa polskiego i europejskiego.
- Dostarczony sprzęt musi być nowy, nie używany wcześniej. Nie dopuszcza się urządzeń odnawianych, demonstracyjnych lub powystawowych.
- Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
- Dostarczone urządzenia muszą być wyprodukowane po 1 stycznia 2022 r.
- Urządzenia muszą być zakupione z oficjalnego kanału dystrybucji na rynek europejski.
- Elementy, z których zbudowane są urządzenia muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta.
- Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
- Pozytywne zakończenie testów wraz z usunięciem wskazanych wad jest niezbędne, aby dla poszczególnych komponentów oraz całego Przedmiotu Zamówienia dokonać odbiorów częściowych i końcowych.

- Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora.
- W przypadku zidentyfikowania błędów lub wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem końcowym Przedmiotu Zamówienia.
- Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych opakowaniach producenta umożliwiających identyfikację zarówno produktu jak i producenta.
- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
- Zamawiający wymaga, aby zaoferowane rozwiązania (systemy, oprogramowanie) były rozwiązaniami istniejącymi, działającymi, gotowymi do wdrożenia i zapewniającymi realizację wszystkich wymaganych w SWZ funkcjonalności na dzień składania ofert i nie mogą być w fazie opracowywania, budowy, testów i projektowania.
- Zamawiający dopuszcza produkty równoważne do opisanych w treści niniejszego dokumentu. Jeżeli zapisy zawarte w Szczegółowym Opisie Przedmiotu Zamówienia wskazywałyby w odniesieniu do rozwiązań, materiałów lub urządzeń znaki towarowe lub pochodzenie Zamawiający dopuszcza składanie ofert na produkty równoważne. Wszelkie produkty pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, jakim musi odpowiadać produkt, aby spełnić wymagania stawiane przez Zamawiającego i stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Poprzez zapis dot. minimalnych wymagań parametrów Zamawiający rozumie wymagania materiałów, sprzętu i urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Tak więc posługiwanie się nazwami producentów (produktów) ma wyłącznie charakter przykładowy. Zamawiający, przy opisie przedmiotu zamówienia, wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych parametrach lub lepszych. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, wykazujących spełnienie przez produkty równoważne ww. parametrów i cech.
- Jeżeli zapisy zawarte w Szczegółowym Opisie Przedmiotu Zamówienia wskazywałyby w odniesienia do norm i standardów w stosunku do urządzeń i oprogramowania Zamawiający dopuszcza normy równoważne.
- W przypadku, gdy w trakcie realizacji Przedmiotu Zamówienia (według zakresu danego pakietu / zadania) okaże się, że z przyczyn niezależnych od Zamawiającego (np. zmiana rozwiązań integracji z Platformą Regionalną, zmian prawnych, zmiana wytycznych dotyczących e-Usług, wymagań CeZ lub Ministerstwa Zdrowia itp.) brakuje jakiegokolwiek urządzenia lub elementu nie ujętego w SWZ, którego brak uniemożliwi prawidłową realizację Przedmiotu Zamówienia, Wykonawca dostarczy je i skonfiguruje tak aby możliwa była realizacja przedmiotu zamówienia na własny koszt.
- Usługi instalacji, konfiguracji i wdrożenia Wykonawca przeprowadzi zgodnie z zapisami niniejszego OPZ w uzgodnieniu z Zamawiającym, zgodnie z obowiązującymi przepisami, zasadami wykonywania projektów teleinformatycznych oraz najlepszymi praktykami w ich realizacji.
- Na całość sprzętu musi być udzielona min. 24 miesięczna gwarancja producenta (chyba, że zapisy szczegółowe stanowią inaczej); serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; podjęcie działań diagnostycznych i kontakt pisemnie lub drogą elektroniczną ze zgłaszającym nie może przekroczyć jednego dnia roboczego.
- Zgłoszenia serwisowe muszą być przyjmowane telefonicznie, przez e-mail lub z wykorzystaniem formularza internetowego.

- Zgłoszenia dotyczące wszystkich urządzeń powinny być przyjmowane w jednym punkcie obsługi zgłoszeń. Przez powyższy punkt rozumie się dedykowany serwis internetowy, telefon lub adres e-mail.
- Na wniosek Zamawiającego Wykonawca zapewni pomoc w awaryjnym odtwarzaniu stanu oprogramowania aplikacyjnego i zgromadzonych danych archiwalnych oraz sprawdzeniu poprawności wykonywania kopii zapasowych oraz zgodności wykonywania kopii bezpieczeństwa z ustalonym harmonogramem.
- Czas naprawy w ramach gwarancji nie może być dłuższy niż 10 dni roboczych. W przypadku gdy wymagany jest dłuższy czas na naprawę, Wykonawca dostarcza na ten czas sprzęt o nie gorszych parametrach funkcjonalnych.
- Wykonawca zapewni dostęp do pomocy technicznej (telefon, e-mail lub formularz internetowy) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań dla pakietów / zadań 3 – 6.
- Oprogramowanie musi posiadać min. 24-miesięczną gwarancję (nie dotyczy silnika bazy danych, poz. 4.2.2 w rozdz. II) liczoną od dnia podpisania protokołu odbioru (w skład której wchodzi zapewnienie poprawności działania, prawo do aktualizacji, zapewnienie wsparcia technicznego), chyba że zapisy szczegółowe stanowią inaczej.
- Wdrożone e-usługi i powiązane z nimi oprogramowanie komunikacyjne i mechanizmy integracyjne z RCIM (np. szyna danych / broker) muszą posiadać min. 48-miesięczną gwarancję liczoną od dnia podpisania protokołu odbioru (w skład której wchodzi zapewnienie poprawności działania, prawo do aktualizacji).

Wdrożone zastosowania muszą być zgodne z wymaganiami określonymi z Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz Ustawy o ochronie danych osobowych.

3. Miejsce instalacji sprzętu i oprogramowania / systemu

Dostarczony sprzęt i oprogramowanie muszą zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części załącznika nr 1 do SWZ, w miejscach wskazanych przez Zamawiającego.

4. Okres wdrożenia oraz wsparcia powdrożeniowego

Przedmiot zamówienia jest podzielony na 6 pakietów / zadań:

- Pakiet / Zadanie nr 1 – Dostarczenie i montaż szafy rack. Termin na realizację pakietu / zadania przez Wykonawcę: 30 dni od daty podpisania umowy z Wykonawcą,
- Pakiet / Zadanie nr 2 – Dostarczenie i montaż klimatyzatora. Termin na realizację pakietu / zadania przez Wykonawcę: 60 dni od daty podpisania umowy z Wykonawcą,
- Pakiet / Zadanie nr 3 – Modernizacja zasilacza awaryjnego UPS. Termin na realizację pakietu / zadania przez Wykonawcę: 90 dni od daty podpisania umowy z Wykonawcą,
- Pakiet / Zadanie nr 4 – Dostarczenie pozostałego sprzętu i oprogramowania wraz z ich pełną konfiguracją lokalną i uruchomieniem oraz modernizacją środowiska serwerowego. Termin na realizację pakietu / zadania przez Wykonawcę: 210 dni od daty zakończenia pakietu / zadania nr 1,
- Pakiet / Zadanie nr 5 – System badań obrazowych – odkładanie do EDM. Termin wykonania: 90 dni od daty zakończenia pakietu / zadania nr 4,

- Pakiet / Zadanie nr 6 – Dostarczenie i uruchomienie modułów HIS, systemu autoryzacji wyników badań laboratoryjnych oraz e-Usług. Termin na realizację pakietu / zadania przez Wykonawcę: 90 dni od daty zakończenia pakietu / zadania nr 4.

Zakończenie pakietów / zadań zostanie potwierdzone podpisaniem przez obie strony protokołu odbioru końcowego. Zamawiający dopuszcza realizację poszczególnych etapów pakietów / zadań za pomocą protokołów odbiorów częściowych. Zamawiający powiadomi Wykonawców następujących po sobie pakietów / zadań o zakończeniu prac pakietów / zadań poprzednich. W przypadku gdyby część regionalna nie została wykonana przed ukończeniem wdrożenia i uruchomienia systemów lokalnych Zamawiający oczekuje uruchomienia e-Usług w terminie 90 dni od gotowości części regionalnej projektu PSIM.

Wykonawcy pakietów / zadań 4, 5 i 6 opracują dla Zamawiającego:

- dokumentację przedwdrożeniową,
- harmonogram wdrożenia,
- dokumentację powdrożeniową.

Dokumentacja powyższa będzie zawierać zapisy opisujące aktualny stan systemów informatycznych Zamawiającego, sposób organizacji prac i realizację przebiegu procesu wdrożenia oraz prace powykonawcze. Harmonogram wdrożenia, przedłożony w terminie do 40 dni od daty podpisania umowy, będzie podlegać akceptacji Zamawiającego oraz warunkuje rozpoczęcie dalszych prac Wykonawcy. Z uwagi konieczność przedstawienia analizy przedwdrożeniowej pakietu / zadania 4, Wykonawcy pakietów / zadań 5 i 6 harmonogram przedłożą w terminie do 90 dni od daty podpisania umowy (po uwzględnieniu informacji zawartych w harmonogramie Wykonawcy pakietu / zadania nr 4).

<u>Zakres dokumentacji dla pakietu / zadania nr 4:</u>

Dokumentacja przedwdrożeniowa powinna zawierać m.in.:

- szczegółowy opis budowy Szpitalnego Systemu Informatycznego (SSI) Zamawiającego,
- analizę migracji danych oraz opis sposobu migracji,
- zakres prac wdrożeniowych wraz z programem migracji danych z SSI,
- szczegółową specyfikację oprogramowania objętego zakresem umowy oraz konfigurację urządzeń i oprogramowania wchodzących w skład SSI,
- analizę wymagań Przedmiotu Zamówienia,
- opis planowanej modernizacji i budowy infrastruktury serwerowej.

Harmonogram wdrożeniowy powinien zawierać w szczególności:

- wyszczególnienie etapów realizacji wraz z terminem ich realizacji,
- termin wykonania migracji danych,
- ustawienia konfiguracyjne urządzeń i sposób przeprowadzania testów,
- harmonogram instruktażu pracowników Zamawiającego z obsługi dostarczonego oprogramowania i sprzętu w zakresie wskazanym przez Zamawiającego,
- plan dostaw,
- opis instalacji i wdrożenia oprogramowania,
- konfigurację i instalację urządzeń sieciowych i serwerowych.

Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powdrożeniowej obejmującej:

- dokumentację użytkową, techniczną i eksploatacyjną,
- szczegółowy opis wykonanych czynności instalacyjnych i konfiguracyjnych komponentów systemu,
- opis zasad wersjonowania i sposobu patchowania aplikacji,
- wyniki przeprowadzonych testów,
- karty katalogowe urządzeń potwierdzające spełnienie wymagań,
- instrukcje obsługi i instrukcje użytkowania dostarczonego oprogramowania,
- charakterystykę licencjonowania wszystkich elementów aplikacji i środowiska,
- opis architektury technicznej (cech charakteryzujących dany typ urządzenia np. serwer, macierz, switche, UTM itp.) wszystkich urządzeń zawierający m.in. adresację sieciową, zainstalowane systemy operacyjne i listę zainstalowanego oprogramowania, zasoby dyskowe, porty sieciowe, zastosowana budowa klastrów,
- opis konfiguracji musi obejmować wszystkie urządzenia wdrożone, zainstalowane będące przedmiotem zamówienia,
- opis architektury logicznej (schemat i opis powiązań logicznych poszczególnych komponentów i ich rolę w architekturze),
- opis czynności administracyjnych dla aplikacji i systemu informatycznego (w postaci procedur lub instrukcji wykonywanych cyklicznie dla utrzymania optymalnej wydajności),
- opis procedury tworzenia i odtwarzania kopii zapasowej wraz z ustalonym harmonogramem wykonywania backupu,
- instrukcję odtworzenia systemów i środowiska informatycznego Zamawiającego po awarii (procedury muszą opisywać kolejne kroki pozwalające na bezpieczne zatrzymanie/uruchomienie elementu infrastruktury hardware'owej oraz aplikacji i elementów infrastruktury software'owej, lub całego środowiska sprzętowo-software'owego),
- opis działań koniecznych do utrzymania wymaganej dostępności i bezpieczeństwa danych,
- wyszczególnienie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- opis struktury zbiorów danych wskazującej zawartość poszczególnych pól informacyjnych i powiązań między nimi,
- informacje o sposobie przepływu danych pomiędzy poszczególnymi systemami,
- opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Dokumentacja powdrożeniowa musi być dostarczona w wersji elektronicznej oraz papierowej.

<u>Zakres dokumentacji dla pakietu / zadania nr 5:</u>

Dokumentacja przedwdrożeniowa powinna zawierać m.in.:

- analizę migracji danych oraz opis sposobu migracji,
- zakres prac wdrożeniowych wraz z programem migracji danych,
- szczegółową specyfikację oprogramowania oraz jego konfigurację,
- analizę wymagań Przedmiotu Zamówienia.

Harmonogram wdrożeniowy powinien zawierać w szczególności:

- wyszczególnienie etapów realizacji wraz z terminem ich realizacji,

- termin wykonania migracji danych,
- ustawienia konfiguracyjne urządzeń i sposób przeprowadzania testów,
- harmonogram instruktażu pracowników Zamawiającego z obsługi dostarczonego oprogramowania,
- opis instalacji i wdrożenia oprogramowania.

Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powdrożeniowej obejmującej:

- dokumentację użytkową, techniczną i eksploatacyjną,
- szczegółowy opis wykonanych czynności instalacyjnych i konfiguracyjnych komponentów systemu,
- opis zasad wersjonowania i sposobu patchowania aplikacji,
- wyniki przeprowadzonych testów,
- instrukcje obsługi i instrukcje użytkowania dostarczonego oprogramowania,
- charakterystykę licencjonowania wszystkich elementów aplikacji i środowiska,
- opis architektury logicznej (schemat i opis powiązań logicznych poszczególnych komponentów i ich rolę w architekturze),
- opis czynności administracyjnych dla aplikacji (w postaci procedur lub instrukcji wykonywanych cyklicznie dla utrzymania optymalnej wydajności),
- opis procedury tworzenia i odtwarzania kopii zapasowej wraz z ustalonym harmonogramem wykonywania backupu,
- instrukcję odtworzenia systemów i środowiska informatycznego Zamawiającego po awarii (procedury muszą opisywać kolejne kroki pozwalające na bezpieczne zatrzymanie/uruchomienie elementu infrastruktury hardware'owej oraz aplikacji i elementów infrastruktury software'owej, lub całego środowiska sprzętowo-software'owego),
- opis działań koniecznych do utrzymania wymaganej dostępności i bezpieczeństwa danych,
- wyszczególnienie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- opis struktury zbiorów danych wskazującej zawartość poszczególnych pól informacyjnych i powiązań między nimi,
- informacje o sposobie przepływu danych pomiędzy poszczególnymi systemami,
- opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności przetwarzanych danych.

Dokumentacja powdrożeniowa musi być dostarczona w wersji elektronicznej oraz papierowej.

<u>Zakres dokumentacji dla pakietu / zadania nr 6:</u>

Dokumentacja przedwdrożeniowa powinna zawierać m.in.:

- zakres prac wdrożeniowych i konfiguracyjnych e-Usług,
- szczegółową specyfikację oprogramowania objętego pakietem / zadaniem oraz konfigurację oprogramowania,
- analizę wymagań Przedmiotu Zamówienia,

Harmonogram wdrożeniowy powinien zawierać w szczególności:

- wyszczególnienie etapów realizacji wraz z terminem ich realizacji,
- instalację i konfigurację e-Usług,

- harmonogram instruktażu pracowników Zamawiającego z obsługi dostarczonego oprogramowania,
- opis instalacji i wdrożenia oprogramowania,

Warunkiem dokonania Odbioru Końcowego jest dostarczenie przez Wykonawcę Dokumentacji Powdrożeniowej obejmującej:

- dokumentację użytkową, techniczną i eksploatacyjną,
- szczegółowy opis wykonanych czynności instalacyjnych i konfiguracyjnych komponentów systemu,
- opis zasad wersjonowania i sposobu patchowania aplikacji,
- wyniki przeprowadzonych testów,
- instrukcje obsługi i instrukcje użytkowania dostarczonego oprogramowania,
- charakterystykę licencjonowania wszystkich elementów aplikacji i środowiska,
- opis architektury logicznej (schemat i opis powiązań logicznych poszczególnych komponentów i ich rolę w architekturze),
- opis czynności administracyjnych dla aplikacji (w postaci procedur lub instrukcji wykonywanych cyklicznie dla utrzymania wymaganej wydajności),
- instrukcję odtworzenia systemów i środowiska informatycznego Zamawiającego po awarii (procedury muszą opisywać kolejne kroki pozwalające na bezpieczne zatrzymanie/uruchomienie elementu infrastruktury hardware'owej oraz aplikacji i elementów infrastruktury software'owej, lub całego środowiska sprzętowo-software'owego),
- opis działań koniecznych do utrzymania wymaganej dostępności i bezpieczeństwa danych,
- wyszczególnienie zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- opis struktury zbiorów danych wskazującej zawartość poszczególnych pól informacyjnych i powiązań między nimi,
- informacje o sposobie przepływu danych pomiędzy poszczególnymi systemami,
- lista wszystkich haseł dostępowych do kont „super użytkowników",
- opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności przetwarzanych danych.

Dokumentacja powdrożeniowa musi być dostarczona w wersji elektronicznej oraz papierowej.

Zamawiający będzie dopuszczony do udziału we wszystkich pracach realizowanych przez Wykonawców w ramach realizacji zamówienia (dostawy, instalacje, konfiguracje, testowanie).
Dla pakietów / zadań 4 – 6 ze strony Wykonawców muszą być wyznaczeni Kierownicy Projektu oraz skład zespołu wdrożeniowego wraz z kontaktem telefonicznym i adresem e-mail.
Wykonawcy zorganizują wdrożenie tak, aby zminimalizować jego wpływ na ciągłość funkcjonowania prac u Zamawiającego. Poszczególne prace będą realizowane etapowo, tak aby zachować ciągłość świadczenia usług medycznych.

W ramach postępowania zostaną przeprowadzone wszystkie testy opisane w dokumentacji. Celem testów jest weryfikacja przez Zamawiającego czy wszystkie prace wykonane w trakcie realizacji Przedmiotu Zamówienia zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiającego jak i wskazanych przez Zamawiającego osób i podmiotów zewnętrznych.

Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad jest niezbędne, aby dla poszczególnych Komponentów oraz całego Przedmiotu Zamówienia dokonać odbiorów w ramach poszczególnych Etapów i Odbioru Końcowego.
Zamawiający ma prawo do weryfikacji należytego wykonania Umowy dowolną metodą, w tym także z wykorzystaniem opinii zewnętrznego audytora. W szczególności uzgodnienie określonych scenariuszy testowych nie wyklucza prawa do weryfikacji prac innymi testami i scenariuszami.
W przypadku zidentyfikowania Błędów lub Wad Wykonawca jest zobowiązany do ich poprawy przed odbiorem Końcowym Przedmiotu Zamówienia.

Odbiór Końcowy Przedmiotu Zamówienia ma na celu potwierdzenie wykonania wszystkich pakietów / zadań wynikających z Umowy, w tym odebrania wszystkich etapów wdrożenia oraz dostarczenia wymaganej zamówieniem Dokumentacji.

Wykonawca pakietu / zadania nr 4 dokona migracji dotychczasowego środowiska SSI na platformę sprzętową dostarczaną w ramach Przedmiotu Zamówienia lub inną wskazaną przez Zamawiającego. Wykonawca ponosi pełną odpowiedzialność za migrowane środowiska oraz zgromadzone dane. Zamawiający wymaga, aby wszystkie istniejące funkcjonalności użytkowanego SSI na dzień podpisania umowy z Wykonawcą zostały zachowane i odtworzone w nowym środowisku.

Wykonawcy, dla pakietów / zadań 4 – 6 przeprowadzą dla osób i w miejscu wskazanym przez Zamawiającego instruktaże stanowiskowe w zakresie elementów środowiska informatycznego wyszczególnionych
w pkt. 6 rozdziału I OPZ. W ramach instruktaży, Wykonawcy przekażą uczestnikom pełną wiedzę niezbędną do poprawnego użytkowania funkcjonalności SSI, oprogramowania i urządzeń. Przeprowadzenie instruktaży zostanie potwierdzone protokołami sporządzonymi w dwóch jednobrzmiących egzemplarzach, po jednym dla Zamawiającego i Wykonawcy, zawierającym:

- zakres instruktażu,
- datę przeprowadzonego instruktażu,
- imienną listę osób uczestniczących,
- imię i nazwisko osób prowadzących instruktaż.

Protokoły z przeprowadzenia instruktaży podlegać będą zatwierdzeniu przez Zamawiającego i będą warunkiem koniecznym do podpisania protokołu Odbioru Końcowego.

Wykonawcy pakietów / zadań 4 – 6 zobowiązani będą do objęcia przedmiotu zamówienia bezpłatnym wsparciem powdrożeniowym. Wykonawcy na potrzebę ewidencjonowania niepożądanych zdarzeń i błędów wymagających obsługi serwisowej udostępnią Zamawiającemu dedykowany serwis internetowy, telefon oraz adres e-mail. Powyższe wsparcie będzie rozumiane jako korygowanie nieprawidłowego działania oprogramowania i sprzętu przez pracowników Wykonawcy w okresie 36 miesięcy od daty odbioru końcowego. Asysta będzie polegała również na udzielaniu porad i odpowiedzi na pytania administratorów oraz dokonywania zmian w konfiguracji sprzętu i oprogramowaniu, także wynikających ze zmieniających się przepisów prawa dotyczących wdrożonych u Zamawiającego rozwiązań. Wykonawcy zobowiązują się w wymienionym okresie do monitorowania zmieniających się przepisów prawa mających wpływ na zgodność dostarczonych systemów do tych zasad.

5. e-Usługi

W ramach projektu Podkarpacki System Informacji Medycznej udostępniane są usługi realizowane drogą elektroniczną (przez Internet). Należą do nich:
e-Informacja – jej zadaniem jest udostępnienie informacji o zakresach i dostępności świadczeń zdrowotnych realizowanych przez podmioty lecznicze uczestniczące w projekcie.
e-Rejestracja – zadaniem tej e-Usługi jest umożliwienie pacjentowi zarejestrowanie się na wybrane usługi medyczne za pomocą konta internetowego.
Elektroniczny Rekord Pacjenta (ERP) – zapewnienia wymianę informacji o dokumentacji medycznej pacjentów pomiędzy podmiotami leczniczymi uczestniczącymi w projekcie.
Regionalny Rejestr Danych Ratunkowych (RRDR) – jej celem jest gromadzenie i udostępnianie najbardziej istotnych danych medycznych o pacjentach z punktu widzenia ratownictwa medycznego.
Elektroniczna Platforma Współpracy ZOZ (EPWZOZ) – zadaniem tej e-Usługi jest umożliwienie przekazywania elektronicznych zleceń do uczestniczących w projekcie jednostek opieki zdrowotnej oraz odbiór wyników tych zleceń.
Elektroniczna Platforma Nadzoru (EPN) – jej zadaniem jest zapewnienie wymiany informacji pomiędzy jednostkami opieki zdrowotnej a organami je nadzorującymi i koordynującymi politykę zdrowotną w regionie (jak np. Urząd Marszałkowski Województwa Podkarpackiego).

W ramach projektu „Modernizacja i rozwój e-usług w ramach Podkarpackiego Systemu Informacji Medycznej (PSIM) w SPZOZ w Sanoku" Zamawiający wymaga aktualizacji usług e-Informacja, e-Rejestracja oraz integracji z nową e-usługą o nazwie RREDM (Regionalne Repozytorium Elektronicznej Dokumentacji Medycznej).

Usługa RREDM będzie pozwalała na przekazywanie z lokalnego repozytorium EDM danych medycznych w formacie HL7 CDA oraz elektronicznych danych obrazowych w formacie DICOM i składowanie ich w roli długoterminowego archiwum medycznej dokumentacji elektronicznej.

Ze względu na konieczność integracji z regionalną platformą PSIM/RCIM usługi muszą zostać zrealizowane z uwzględnieniem wymagań integracji z RCIM. Wymagania te zostały przedstawione na stronie konkursu: *https://rpo.podkarpackie.pl/index.php/nabory-wnioskow/2426-2-1-podniesienie-efektywnosci-i-dostepnosci-e-uslug-nr-naboru-rppk-02-01-00-iz-00-18-004-19* (załączniki 11.2 i 11.3).

Dodatkowo szpital z własnych środków wdrożył inne e-usługi:
e-Recepta – integracja HIS z ogólnokrajowym systemem do realizacji e-recept. E-usługa jest częścią Internetowego Konta Pacjenta (IKP - pacjent.gov.pl). Dzięki niej pacjenci mogą pobrać, przeglądać, a przede wszystkim realizować recepty. Poziom dojrzałości 3.

KOWAL – narzędzie ułatwiające i zwiększając komfort zarządzania informacjami o obrocie lekami w ramach Apteki Szpitalnej, której obsługa realizowana jest za pomocą systemu AMMS. Nadrzędną funkcją prezentowanego narzędzia jest weryfikacja autentyczności leków i wycofywania unikalnych identyfikatorów opakowań z centralnego systemu baz Europejskiego Systemu Weryfikacji Leków poprzez Polski Narodowy Systemem Weryfikacji Leków (PLMVS). Poziom dojrzałości 1.

ZSMOPL – Głównym celem usługi jest usprawnienie procesów biznesowych związanych z dostępem do informacji o obrocie produktami leczniczymi. Zintegrowany System Monitorowania Obrotu Produktami Leczniczymi umożliwia m.in. monitorowanie na poziomie detalicznym i hurtowym obrotu lekami oraz przekazywanie tych informacji do właściwych organów. Do podstawowych funkcjonalności tego systemu należy zaliczyć gromadzenie, przetwarzanie i udostępnianie danych dotyczących obrotu produktami monitorowanymi w tym:

- produktami leczniczymi dopuszczonymi do obrotu na terytorium RP,
- refundowanymi wyrobami medycznymi i środkami specjalnego przeznaczenia żywieniowego dopuszczonymi do obrotu na terytorium RP,

- produktami leczniczymi pochodzącymi z importu docelowego i interwencyjnego.

TOPSOR – Tryb Obsługi Pacjenta w SOR tworzy wystandaryzowany system rejestracji i przyjęć pacjentów w Szpitalnym Oddziale Ratunkowym. Zgodnie z założeniami projektu w szpitalnym oddziale ratunkowym prowadzona jest segregacja medyczna, która odbywa się za pomocą systemu zarządzającego trybem obsługi pacjenta. System umożliwia łatwy dostęp do informacji o przewidywanym czasie oczekiwania jak również usprawnia pracę SOR w celu zwiększenia efektywności udzielanych świadczeń zdrowotnych.

Zamawiający wymaga aby wszystkie obecnie działające u niego usługi i systemy zostały poprawnie skonfigurowane i uruchomione w nowym środowisku.

5.1. Opis usługi e-Informacja

Funkcjonalności e-Informacji umożliwiają:
- dostęp do informacji dotyczących opieki zdrowotnej,
- korzystanie z Informatora o usługach medycznych,
- wyszukiwanie usług medycznych realizowanych przez jednostki opieki zdrowotnej w regionie Podkarpacia,
- zakładanie i obsługę konta użytkownika końcowego, a także korzystanie z funkcjonalności dostępnych dla zalogowanych użytkowników,
- integrację danych.

Usługa e-Informacja jest oprogramowaniem aplikacyjnym (portalem www) zlokalizowanym w warstwie regionalnej PSIM. Dostęp do funkcjonalności publikującej informacje dotyczące opieki zdrowotnej oraz usług medycznych realizowanych przez zintegrowane z RCIM jednostki opieki zdrowotnej jest możliwy poprzez przeglądarkę internetową i nie wymaga logowania.
W przypadku korzystania z treści, takich jak informacje ogólne dla pacjenta, Aktualności, Karta Praw Pacjenta, informacje o regulacjach prawnych pochodzące z dedykowanych serwisów informacyjnych lub katalog plików do pobrania użytkownik wybiera odpowiednią opcję z udostępnionych w ramach portalu www e-Informacja.
Informacje o usługach medycznych, dostępnych w jednostkach ochrony zdrowia zintegrowanych w ramach PSIM, są prezentowane z zasobów RCIM. W warstwie regionalnej gromadzone są dane o jednostkach ochrony zdrowia, ich strukturze organizacyjnej, usługach realizowanych przez poszczególne jednostki, o personelu realizującym usługi w danej jednostce ochrony zdrowia oraz o pierwszym wolnym terminie, na który można wykonać rejestrację na daną usługę. Wymienione informacje są zebrane w postaci katalogów:
- Katalog Jednostek Ochrony Zdrowia,
- Katalog Usług,
- Katalog Personelu.

Podczas przeglądania danych o usługach medycznych przy każdej z usług występuje opcja umożliwiająca, poprzez jedno kliknięcie, przejście do usługi e-Rejestracja i rezerwację terminu wizyty.
Użytkownik ma możliwość wyszukiwania usług medycznych w prowadzonych w warstwie regionalnej Katalogach danych. Warstwa regionalna PSIM, po wyszukaniu danych spełniających określone kryteria w odpowiednich katalogach, prezentuje je użytkownikowi. Dla każdej z wyszukanych usług medycznych dostępna jest informacja o orientacyjnym pierwszym wolnym terminie Rejestracji.

Rozróżniane są 3 rodzaje usług:

- dostępne do e-Rejestracji – na które możliwa jest rejestracja elektroniczna,
- oferowane – które są wyłącznie prezentowane na portalu bez możliwości rejestracji elektronicznej,
- wewnętrzne – dostępne wyłącznie do zleceń pomiędzy podmiotami w ramach e-Usługi EPW-ZOZ.

Każda wyświetlona w wynikach wyszukiwania usługa medyczna dostępna do e-Rejestracji posiada opcję umożliwiającą przejście do usługi e-Rejestracja i rezerwację terminu wizyty, jeśli lokalny udostępnił grafik przyjęć dla tek usługi.
W ramach funkcjonalności usługi istnieje możliwość założenia konta użytkownika końcowego w systemie PSIM. Zalogowanym użytkownikom końcowym dostarczane są dodatkowe funkcjonalności. Są to m.in.: obsługa otrzymywanych i wysyłanych wiadomości systemowych, rejestrowanie i obsługa subkont przez opiekunów (np. rodzica dziecka, przedstawiciela ustawowego), konfiguracja własnego konta (np. dane kontaktowe), a także dostęp i wizualizacja dla funkcjonalności innych e-Usług (np. e-Rejestracja, przeglądanie i wprowadzanie dodatkowych danych ratunkowych).
Funkcjonalność zakładania konta użytkownika końcowego i logowania się jest dostępna na portalu www i jej użycie nie wymaga logowania. Funkcjonalności dotyczące obsługi konta wymagają autoryzacji.
Regionalne katalogi danych w RCIM są zasilane danymi z lokalnych systemów medycznych HIS w zakresie wymaganym do prezentacji aktualnej informacji w ramach usługi e-Informacja. Zasilenie odbywa się za pomocą udostępnianych interfejsów o zdefiniowanej strukturze. Zasilanie rozpoczyna się w momencie automatycznego uruchomienia procesu ładowania, wynikającego z częstotliwości zasilania zdefiniowanej w Module Administracji Regionalnej. Warstwa regionalna przekazuje żądanie synchronizacji danych do poszczególnych jednostek ochrony zdrowia. W każdej z jednostek system lokalny udostępnia przygotowane dane portalowe. RCIM weryfikuje poprawność danych i dokonuje zapisu w odpowiednich katalogach.

Wykonawca zobowiązany jest do modyfikacji usługi pod kątem wymagań PSIM II.

5.2. Opis usługi e-Rejestracja

Funkcjonalności e-Rejestracji umożliwiają:
- Rezerwację usług medycznych w jednostkach ochrony zdrowia zintegrowanych z RCIM za pośrednictwem portalu internetowego przez zarejestrowanych na poziomie regionalnym użytkowników końcowych (pacjentów),
- Anulowanie wskazanej na liście rejestracji,
- Śledzenie zdarzeń związanych z rejestracją za pomocą systemu komunikatów (powiadomień) dla użytkowników końcowych, w formie wiadomości e-mail i SMS, dotyczących: potwierdzenia rejestracji, zbliżającego się terminu wizyty, anulowania wizyty oraz zmiany terminu wizyty.

Użytkownik ma możliwość rezerwacji terminu wizyty na wybraną usługę medyczną, wykonywaną przez jednostkę ochrony zdrowia, za pomocą usługi internetowej udostępnianej na portalu e-Informacja lub na lokalnym portalu internetowym jednostki ochrony zdrowia.
Z e-Rejestracji mogą korzystać wyłącznie zarejestrowani na poziomie regionalnym użytkownicy końcowi. W celu wykonania rejestracji użytkownik musi być zalogowany do konta użytkownika końcowego umiejscowionego w warstwie regionalnej RCIM. Logowanie odbywa się za pomocą jednej z funkcjonalności usługi e-Informacja.
Użytkownik rozpoczyna rezerwację terminu wizyty od wyszukania i wybrania odpowiedniej usługi medycznej realizowanej we wskazanej jednostce ochrony zdrowia. Odbywa się to w ramach funkcjonalności usługi e-Informacja. Użytkownik wskazuje wolny termin, z dokładnością do dnia i godziny, oraz – w zależności od usługi i jednostki ochrony zdrowia – konkretny personel lub konkretne miejsce wykonania usługi. W warstwie RCIM następuje walidacja kolizji rezerwacji polegająca na

sprawdzeniu, czy istnieją wielokrotne rezerwacje różnych usług jednego dnia na tę samą godzinę, co wskazany termin. Następnie warstwa regionalna PSIM przekazuje do odpowiedniej jednostki ochrony zdrowia żądanie zablokowania wskazanego terminu wizyty w systemie medycznym. System lokalny blokuje wskazany termin jest na określony czas. Termin wizyty jest odblokowywany w przypadku przerwania sesji lub braku potwierdzenia przez użytkownika rezerwowanej wizyty na zakończenie dokonywania rezerwacji. Następnie użytkownik wprowadza dane wymagane do rejestracji na wyświetlonym przez system regionalny formularzu rejestracji i zatwierdza je. Przed przekazaniem danych do warstwy lokalnej system regionalny weryfikuje poprawność wypełnienia formatki rejestracji i kompletność wymaganych danych. Jeżeli dane są poprawne, to system regionalny wysyła je do odpowiedniej jednostki ochrony zdrowia w celu zarejestrowania pacjenta. Jeżeli nie można wykonać rejestracji, to system lokalny przekazuje do RCIM informację o jej odrzuceniu i zwalnia wstępną rezerwację wybranego terminu, a warstwa regionalna informuje użytkownika o odrzuceniu rezerwacji terminu wizyty. Jeżeli pacjent może zostać zarejestrowany, to system lokalny dokonuje wstępnej rezerwacji wizyty w podanym terminie i przekazuje do RCIM potwierdzenie zaplanowania rejestracji. Warstwa regionalna informuje użytkownika o przyjęciu rezerwacji terminu wizyty wyświetlając odpowiedni komunikat na ekranie, zapisuje rejestrację w danych przechowywanych na koncie użytkownika oraz wysyła do użytkownika końcowego powiadomienia potwierdzające rejestrację. System lokalny zmienia wówczas status rezerwacji z zaplanowanej na potwierdzoną.

Użytkownik końcowy może zrezygnować z terminu zaplanowanej wizyty, czyli anulować rejestrację w lokalnym systemie medycznym. Anulowanie wizyty jest możliwe z poziomu e-usługi e-Informacja.

W celu anulowania rejestracji użytkownik musi być zalogowany do swojego konta. Anulowanie terminu wizyty odbywa się poprzez wskazanie wybranej rezerwacji i wybranie odpowiedniej opcji. W efekcie system lokalny anuluje wskazaną rejestrację i przekazuje do warstwy regionalnej potwierdzenie anulowania, system regionalny zmienia status rejestracji w RCIM i zapisuje odpowiedni status na koncie użytkownika oraz powiadamia go o anulowaniu terminu wizyty.

W ramach usługi e-Rejestracja funkcjonuje system powiadomień dla użytkowników końcowych w formie wiadomości e-mail i SMS wysyłanych automatycznie z RCIM w przypadku wystąpienia następujących zdarzeń:

- potwierdzenia rejestracji,
- zbliżającego się terminu wizyty,
- anulowania wizyty,
- zmiany terminu wizyty (zarówno przez użytkownika jak i w lokalnym systemie medycznym HIS).

Powiadomienia SMS i e-mail są obsługiwane dla wszystkich sposobów rejestracji (poprzez www, telefon, osobiście) dla użytkowników posiadających konto Użytkownika Końcowego. Sposób powiadamiania – wysyłanie wiadomości e-mail lub wiadomości SMS lub wysyłanie obydwu rodzajów wiadomości – zależy od konfiguracji wykonanej w Module Administracji Regionalnej oraz parametryzacji konta użytkownika końcowego. Zawartość komunikatu również jest definiowana w MAR niezależnie dla każdego rodzaju zdarzenia i składa się z części stałej oraz danych dotyczących konkretnego zdarzenia (termin wizyty, imię i nazwisko pacjenta itp.).

Po otrzymaniu przez warstwę regionalną informacji o zakończeniu wizyty w lokalnym systemie medycznym, system regionalny zmienia status rejestracji w RCIM w danych gromadzonych na koncie użytkownika końcowego.

W ramach usługi e-Rejestracja używane są formularze do wprowadzania danych umożliwiających rezerwację terminu wizyty w lokalnych systemach medycznych jednostek ochrony zdrowia zintegrowanych z RCIM.

Zawartość formularzy może być różna dla danego typu usługi medycznej w poszczególnych jednostkach ochrony zdrowia – może być różny zakres danych do uzupełnienia przez Pacjenta. Wobec tego poszczególne formatki mogą zawierać różne pola służące do wprowadzania danych.

- formularzami e-Rejestracji zarządza Administrator RCIM,
- formularz przypięty jest do każdej usługi zdefiniowanej przez Podmiot Leczniczy, która została zasilona do RCIM,
- formularz może być domyślny lub dedykowany,
- standardowo, do każdej usługi podpięty jest formularz domyślny,
- formularz domyślny zawiera sekcję podstawową: informacje o usłudze i pole Numer telefonu kontaktowego pacjenta,
- formularz dedykowany posiada sekcję podstawową (niezmienną) oraz sekcję dodatkową (definiowaną przez użytkownika),
- ilość formularzy dedykowanych nie jest ograniczona i zależy od użytkownika.

Na liście rejestracji prezentowane są nie tylko te wizyty, na które rejestracje zostały wykonane za pomocą portalu internetowego, ale również te, które pacjent umówił osobiście lub telefonicznie w podmiocie leczniczym. Mogą być widoczne również rejestracje do usług, dla których nie udostępniono grafików na portalu internetowym. Warunkiem jest ustawienie dostępności e-Rejestracji dla danej usługi.
Rekomendowane jest udostępnienie e-Rejestracji dla wszystkie usług medycznych, oprócz usług wrażliwych (np. w Poradniach Psychiatrycznych, Uzależnień, itp.) oraz tych, dla których nie ma możliwości rejestracji (np. w przypadku usług z jednostką statystyczną Pobyt, Pobyt w oddziale szpitalnym, Wyjazd ratunkowy czy Cykl leczenia).

Wykonawca zobowiązany jest do modyfikacji usługi pod kątem wymagań PSIM II.

5.3. Opis usługi ERP – Elektroniczny Rekord Pacjenta

e-Usługa ERP umożliwia:
- wyszukiwanie elektronicznej dokumentacji medycznej (EDM) pacjenta zlokalizowanej w jednostkach opieki zdrowotnej zintegrowanych z RCIM,
- prezentację wyników wyszukiwania tej dokumentacji,
- pobranie elektronicznego dokumentu wskazanego z listy wyników wyszukiwania dokumentacji,
- prezentację danych elektronicznej dokumentacji medycznej.

Po zalogowaniu się do e-Usługi użytkownik precyzuje kryterium wyszukiwania elektronicznej dokumentacji medycznej pacjenta. System (RCIM) weryfikuje czy pacjent złożył zgodę na udostępnianie elektronicznej dokumentacji medycznej i jakich jednostek opieki zdrowotnej ta zgoda dotyczy. Następnie system komunikuje się z poszczególnymi jednostkami przekazując do każdej z nich żądanie wyszukania Elektronicznej Dokumentacji Medycznej (EDM) pacjenta. Komunikacja z każdą jednostką odbywa się wg zdefiniowanego interfejsu wymiany danych. Jednostki zintegrowane z RCIM (na wskutek pojawienia się żądania) wyszukują wg przekazanego kryterium wyszukiwania w swoich systemach elektroniczną dokumentację medyczną pacjenta, a wynik wyszukiwania przekazują do RCIM. e Usługa ERP odbiera i przetwarza wyniki przekazane przez odpytane jednostki w celu zaprezentowania użytkownikowi. W przypadku, gdy dana jednostka nie jest dostępna (np. brak połączenia z jednostką), do zbioru wyników dodawana jest informacja o braku komunikacji z jednostką, a w związku z tym braku informacji czy w danej jednostce istnieje EDM pacjenta wskazanego w kryterium wyszukiwania. Następnie zbiór wynikowy jest wyświetlany użytkownikowi, a ten zapoznaje się z informacjami. W przypadku, gdy istnieje elektroniczna dokumentacja pacjenta spełniająca kryterium wyszukiwania (wyświetlana jest lista pozycji) użytkownik może pobrać EDM wybierając odpowiedni link. e Usługa komunikuje się z odpowiednim systemem danej jednostki opieki zdrowotnej, w którym jest zlokalizowana elektroniczna dokumentacja, pobiera dokumentację i prezentuje ją użytkownikowi. Dodatkowo system umożliwia zapisanie pobranej

elektronicznej dokumentacji w systemie jednostki opieki zdrowotnej użytkownika wyszukującego dane.
Dokumenty w formacie DICOM, ze względu na objętość, są przesyłane do jednostki przeglądającej dokumentację medyczną pacjenta, tylko w przypadku jawnego żądania użytkownika utworzenia lokalnej kopii dokumentu (w przeglądającej/pobierajacej jednostce).
Oglądanie i przetwarzanie takich dokumentów jest możliwe bez potrzeby tworzenia ich pełnej lokalnej kopii. W związku z tym wymogiem jest, aby każdy Podmiot Leczniczy zintegrowany z PSiM, który przechowuje dokumenty DICOM, udostępniał je zgodnie ze standardem WADO (Web access to DICOM object).

Wykonawca zobowiązany jest do utrzymania integracji usługi pod kątem wymagań PSIM II.

5.4. Opis usługi EPW-ZOZ – Elektroniczna Platforma Współpracy ZOZ

Funkcjonalności EPW umożliwiają:

- rejestrowanie, edycję i usuwanie umów pomiędzy dwoma podmiotami leczniczymi na zlecanie przez dany podmiot leczniczy usług medycznych realizowanych przez drugi podmiot leczniczy,
- wprowadzanie i przekazywanie zleceń do innych jednostek ZOZ obejmujących usługi zawarte na umowach,
- anulowanie zleceń przez zlecającego i realizującego,
- przyjęcie lub odrzucenie zlecenia przez jednostkę realizującą,
- przesłanie przez realizatora wyników zleceń,
- odbiór wyników,
- odbiór informacji zwrotnych.

Aby było możliwe zlecanie usług do innych ZOZ, należy wprowadzić do regionalnego katalogu umów odpowiednie umowy zawarte między jednostkami. Do wprowadzania, edycji, usuwania i przeglądania umów służą dedykowane formatki działające w RCIM. Dostęp do formatek realizowany jest przez przeglądarkę internetową.
Użytkownik wprowadza w warstwie regionalnej umowę zawartą między jednostkami, określającą usługi, które jedna jednostka może zlecić w drugiej jednostce. Na umowie zapisywane są również mapowania usług na usługi po stronie zlecającego. Możliwa jest późniejsza edycja umowy oraz jej usunięcie. Po wprowadzeniu, modyfikacji lub usunięciu umowy przez użytkownika jednego ZOZ, operacja jest zatwierdzana przez pracownika drugiego ZOZ. Umowa zaczyna obowiązywać od momentu jej zatwierdzenia.
System warstwy lokalnej pobiera umowy za pomocą interfejsu udostępnianego przez warstwę regionalną. Dzięki temu możliwe jest tworzenie zleceń zgodnych z umowami zapisanymi w RCIM.
Pracownik medyczny ZOZ wprowadza zlecenie na realizację usług objętych umową z innym ZOZ zintegrowanym z RCIM. Zlecenie może obejmować wiele usług. Warstwa regionalna weryfikuje zlecenie i w przypadku braku błędów przekazuje je do jednostki realizującej. Weryfikacja dotyczy zgodności z rejestrem umów oraz poprawności składniowej.
Następnie zlecenie trafia do ZOZ realizującego. Jest zapisywane w tamtejszym systemie HIS i otrzymuje identyfikator unikalny w ramach jednostki realizującej. System wysyła potwierdzenie odebrania zlecenia. Zlecenie trafia na listę zleceń odebranych.
Pracownik ZOZ, do którego trafiło zlecenie decyduje o przyjęciu lub odrzuceniu zlecenia. Wysyłana jest informacja zwrotna zawierająca dla każdej zleconej usługi informację o przyjęciu do realizacji wraz z terminem planowanej realizacji, lub informację o odmowie realizacji usługi wraz z powodem odmowy.
Zlecenie jest przekazywane do odpowiednich jednostek realizujących w ramach ZOZ. Po zrealizowaniu usług przygotowywane i przesyłane są wyniki zlecenia. Jednorazowo mogą być wysłane wyniki wielu

usług, ale niekoniecznie wszystkich zleconych usług, ponieważ usługi mogą być realizowane w różnych terminach i przez różne jednostki wewnętrzne usługodawcy realizującego.
Z każdą usługą na zleceniu jest związany status. Zmienia się on na każdym etapie obsługi zlecenia – system jednostki realizującej przekazuje informacje o zmianie statusu usług.
Zlecenie może zostać anulowane przez zlecającego lub realizującego. Jeśli zlecenie anuluje zlecający, wówczas realizujący musi potwierdzić anulowanie. Żądanie anulowania przesłane przez zlecającego dotyczy całego zlecenia. Potwierdzenie anulowania jest informacją o zmianie statusu usług i określa, które usługi zostały anulowane (nie można anulować usług zrealizowanych oraz tych, których realizacja się rozpoczęła i nie można z niej zrezygnować). Jeśli anulującym jest realizator zlecenia, wówczas przesyła on tylko informację o zmianie statusu wybranych usług na anulowane.
Proces kończy się, gdy zlecający odbierze wyniki wszystkich zleconych i nieanulowanych usług.

Wykonawca zobowiązany jest do utrzymania integracji usługi pod kątem wymagań PSIM II.

5.5. Opis usługi RREDM – Regionalne Repozytorium EDM

Usługa RREDM (Regionalne Repozytorium Elektronicznych Danych Medycznych) jest nową usługą, która nie funkcjonowała dotychczas na platformie PSIM. E-usługa polegać będzie na udostępnieniu podmiotom leczniczym (zintegrowanym z PSIM) możliwości przechowywania kopii elektronicznej dokumentacji medycznej. Dzięki tej e-usłudze zostanie zwiększone bezpieczeństwo podmiotów leczniczych w zakresie ochrony przed utratą elektronicznej dokumentacji medycznej np. w wyniku awarii lokalnych systemów informatycznych lub lokalnej infrastruktury serwerowej.

Usługa będzie pozwalała na składowanie w RREDM kopii elektronicznych dokumentów medycznych (format HL7 CDA) oraz elektronicznych danych obrazowych, będących wynikiem badań obrazowych, pacjentów (format DICOM) przekazanych z Lokalnego Repozytorium Danych Medycznych (LREDM). Poszczególne podmioty lecznicze będą miały dostęp do indywidualnych wskazanych zasobów/zbiorów zlokalizowanych w centrum regionalnym PSIM.
Umożliwienie składowania elektronicznych danych pozwoli też podmiotom leczniczym na wykorzystanie RREDM w roli długoterminowego archiwum, co z kolei przyczyni się do zmniejszenia wymogów sprzętowych, w podmiotach, związanych z zapewnieniem archiwum dokumentacji elektronicznej.
Przekazywane przez podmioty dokumenty będą klasyfikowane ze względu na wymagany okres przechowywania, pozwoli to na wprowadzenie mechanizmów po stronie e-usługi kontrolujących terminowości przechowywania i niszczenia (usuwania) przeterminowanej dokumentacji medycznej pacjentów.

Wykonawca zobowiązany jest do integracji z nową usługą RREDM pod kątem wymagań PSIM II.

6. Zakres przedmiotu zamówienia

Przedmiot zamówienia podzielony został na 6 pakietów / zadań.

6.1. Pakiet / Zadanie nr 1. Dostarczenie i montaż szafy rack.

W ramach pakietu / zadania planuje się zakup i montaż szafy serwerowej o wysokości (U) 42U. Szerokość i głębokość to odpowiednio 800 mm i 1000 mm. Parametry techniczne znajdują się w rozdziale II, punkt 1. Termin realizacji pakietu / zadania to 30 dni od daty podpisania umowy z Wykonawcą.

6.2. Pakiet / Zadanie nr 2. Dostarczenie i montaż klimatyzatora.

W ramach pakietu / zadania planuje się zakup i montaż ściennego klimatyzatora o mocy min. 5 kW. Parametry techniczne urządzenie znajdują się w rozdziale II, punkt 2. Termin realizacji pakietu / zadania to 60 dni od daty podpisania umowy z Wykonawcą.

6.3. Pakiet / Zadanie nr 3. Modernizacja zasilacza awaryjnego UPS.

W ramach pakietu / zadania planuje się wymianę 36 sztuk baterii w posiadanym przez Zamawiającego urządzeniu UPS Eaton 9355-20-N-MBS. Wymagania jakościowe określono w rozdziale II, punkt 3. Termin realizacji pakietu / zadania to 90 dni od daty podpisania umowy z Wykonawcą.

6.4. Pakiet / Zadanie nr 4. Dostarczenie pozostałego sprzętu i oprogramowania wraz z ich pełną konfiguracją lokalną i uruchomieniem oraz modernizacją środowiska serwerowego.

Parametry techniczne dostarczanych urządzeń i oprogramowania znajdują się w rozdziale II, punkt 4. Termin realizacji pakietu / zadania to 210 dni od daty zakończenia pakietu / zadania nr 1.

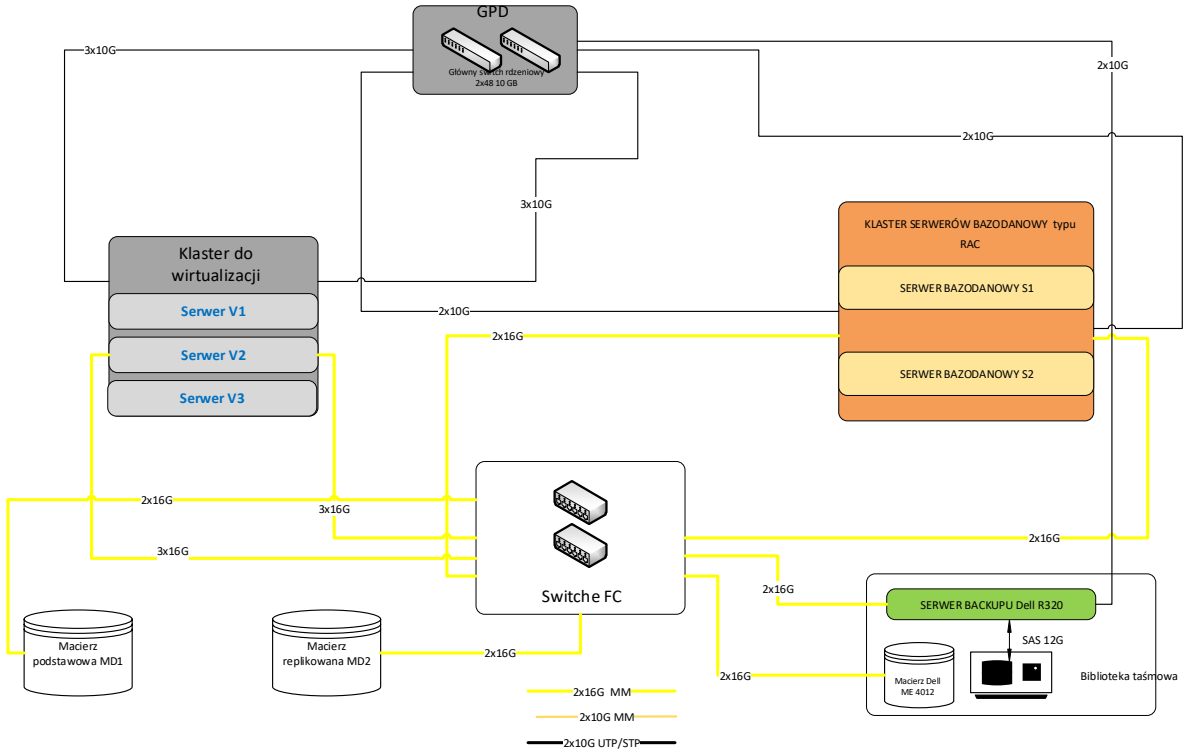
6.4.1. Wymagania Zamawiającego w zakresie prowadzonej modernizacji

Wymagania Zamawiającego w zakresie prowadzonej modernizacji:

- Zamawiający wymaga, aby obecna infrastruktura sprzętowa, programowa oraz licencje zostały wykorzystana w maksymalnym stopniu.
- Zamawiający wymaga, aby Wykonawca zachował kompatybilność z obecną infrastrukturą lub jeśli nie będzie to możliwe dokona modyfikacji infrastruktury na swój koszt.
- Zamawiający wymaga, aby Wykonawca zapewnił zgodność modernizacji z założeniami projektu Podkarpackiego Systemu Informacji Medycznej (PSIM) oraz zachował ciągłość trwania posiadanej przez Zamawiający gwarancji udzielonej przez wykonawcę projektu PSIM na obecną infrastrukturę dostarczoną w ramach projektu PSIM.
- Zamawiający wymaga, aby kompleksowa przebudowa architektury systemu w części serwerowej umożliwiła dalszą rozbudowę oraz separację podsystemów, zwłaszcza podsystemu bazodanowego.
- Zamawiający wymaga, aby Wykonawca wdrożył mechanizmy wysokiej dostępności na poziomie sprzętowym (redundancja, replikacja) oraz systemowym i bazodanowym (klastry odpornościowe), wskazane w projekcie Podmiotu medycznego.
- Wykonawca przeprowadzi aktualizację oprogramowania sprzętowego/układowego (firmware), wskazanych przez Zamawiającego urządzeń, do najwyższej dostępnej stabilnej wersji jednakże przy zachowaniu kompatybilności z innymi elementami infrastruktury.
- Wykonawca przeprowadzi aktualizację oprogramowania systemowego do najwyższej dostępnej i stabilnej wersji, przy zachowaniu zgodności z posiadaną lub dostarczaną licencją do Podmiotu medycznego oraz zgodnie z wytycznymi producenta oprogramowania instalowanego na tychże systemach.

6.4.2. Wdrożenie środowiska macierzowego wysokiej dostępności (HA), sieć SAN

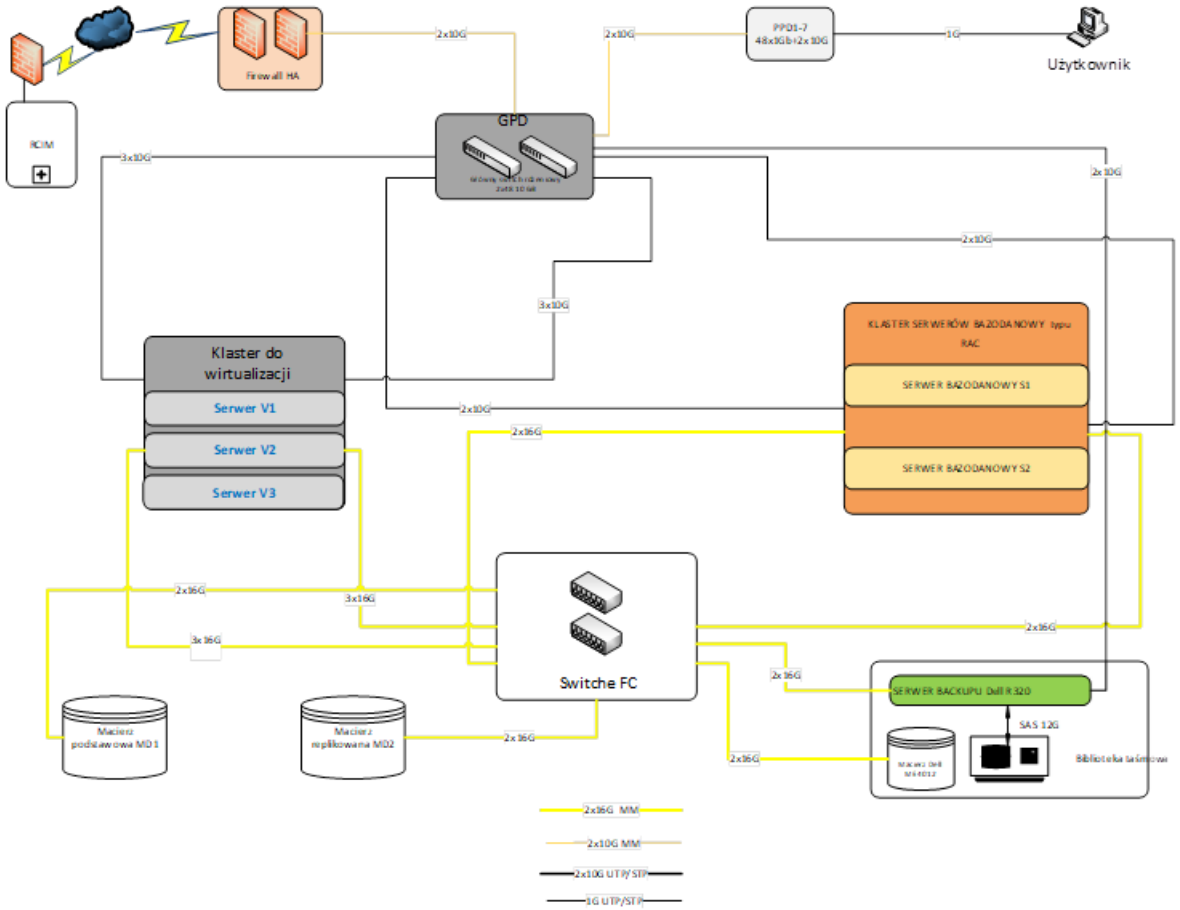
- Środowisko będzie zbudowane w oparciu o klaster wysokiej dostępności składający się z dwóch serwerów-hostów z zainstalowanym oprogramowaniem do wirtualizacji. Dwa serwery bazodanowe S1 i S2, wyposażone w 2 portowe karty FC 16G przeznaczone będą dla potrzeb silnika bazy danych.
- Wysoką dostępność zapewnia zastosowanie dwóch macierzy dyskowych podłączonych do serwerów z wykorzystaniem przełączników FC. Zastosowane zostaną dwa przełączniki celem zapewnienia wymaganej redundancji połączeń.
- Macierz MD1 wyposażona zostanie szybkie dyski SSD.
- Druga macierz MD2 zainstalowana w serwerowni zapasowej za pomocą mechanizmów replikacji synchronicznej będzie kopią lustrzaną macierzy MD1.
- Obecnie użytkowany serwer Dell R320 i istniejąca macierz Dell ME 4012 wykorzystane będą jako przestrzeń do systemu backup typu „disc to disc", dodatkowo dane archiwizowane będą na bibliotece taśmowej w standardzie LTO8.



Rys. Schemat połączeń SAN.

6.4.3. Zwiększenie przepustowości szkieletu sieci do 10G

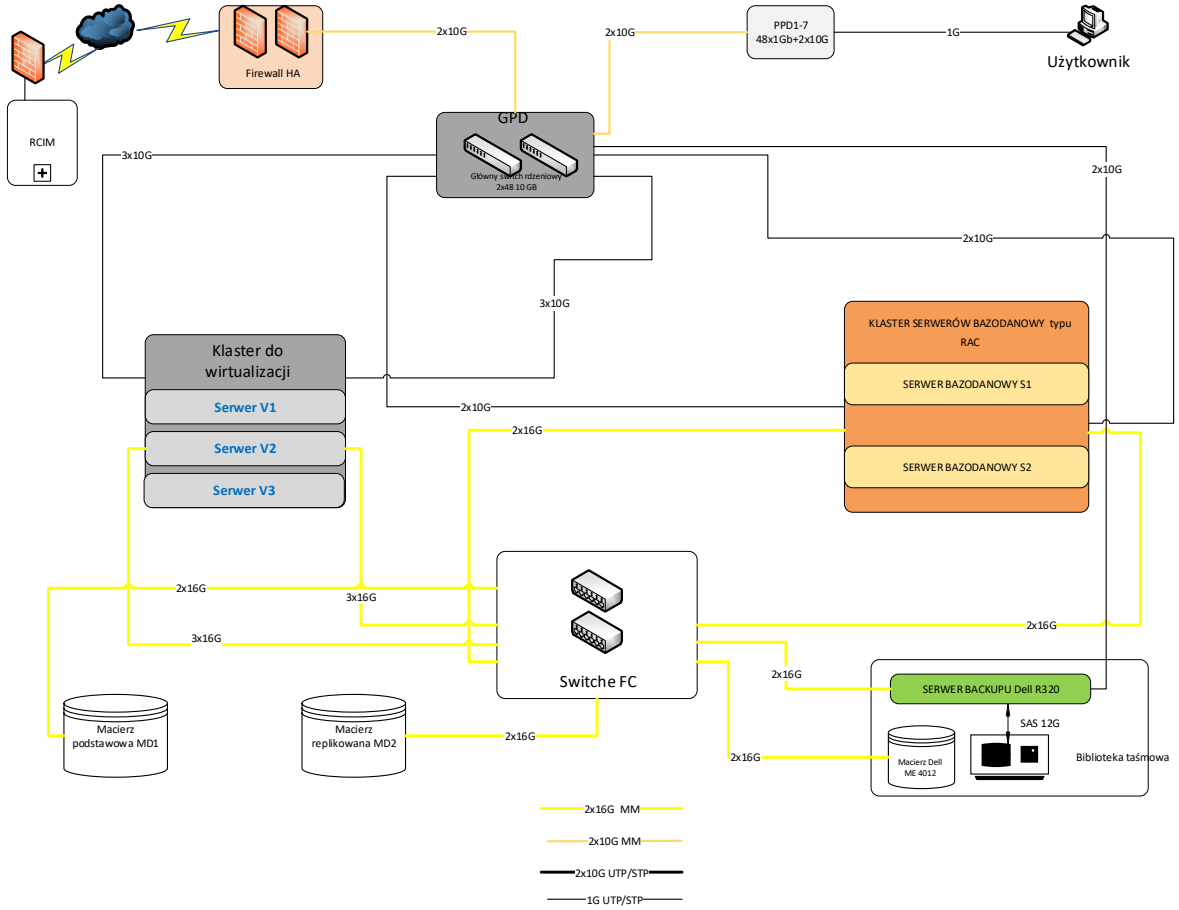
Zakłada się przebudowę szkieletu sieci LAN poprzez wymianę przełączników rdzeniowych z istniejących 1G na standard 10G. Przełączniki dystrybucyjne doposażone będą w 2 moduły SFP+ 10G. Każdy PPD Pośredni Punkt Dystrybucyjny połączony będzie z GPD (Główny Punkt Dystrybucyjny) dwoma torami światłowodowymi o przepustowości 10G zapewniającymi redundancję połączeń oraz przełączników dystrybucyjnych z przełącznikami rdzeniowymi realizowane będzie dwoma torami.



Rys. Schemat połączeń sieci SAN i LAN w obrębie środowiska serwerowego.

6.4.4. Wirtualizacja środowiska serwerowego

Planuje się zbudowanie klastra wirtualizacji składającego się z 3 serwerów fizycznych o jednakowej konfiguracji. Dostarczony system do budowy klastra wirtualizacyjnego powinien zawierać licencje min. dla 6 procesorów. Każdy z 3 serwerów połączony będzie do sieci LAN (poprzez switche rdzeniowe) podwójnym łączem 10G, jeden tor do jednego switcha rdzeniowego drugi tor do drugiego switcha rdzeniowego (redundancja połaczeń). Serwery klastra wirtualizacyjnego będą również połączone do sieci SAN łączami FC 16G 2x16G do switchy FC dającym redundantne połączenia do zasobów macierzowych. Planuje się utworzenie kilkunastu maszyn wirtualnych z różnymi systemami MS WinSRV, Linux.

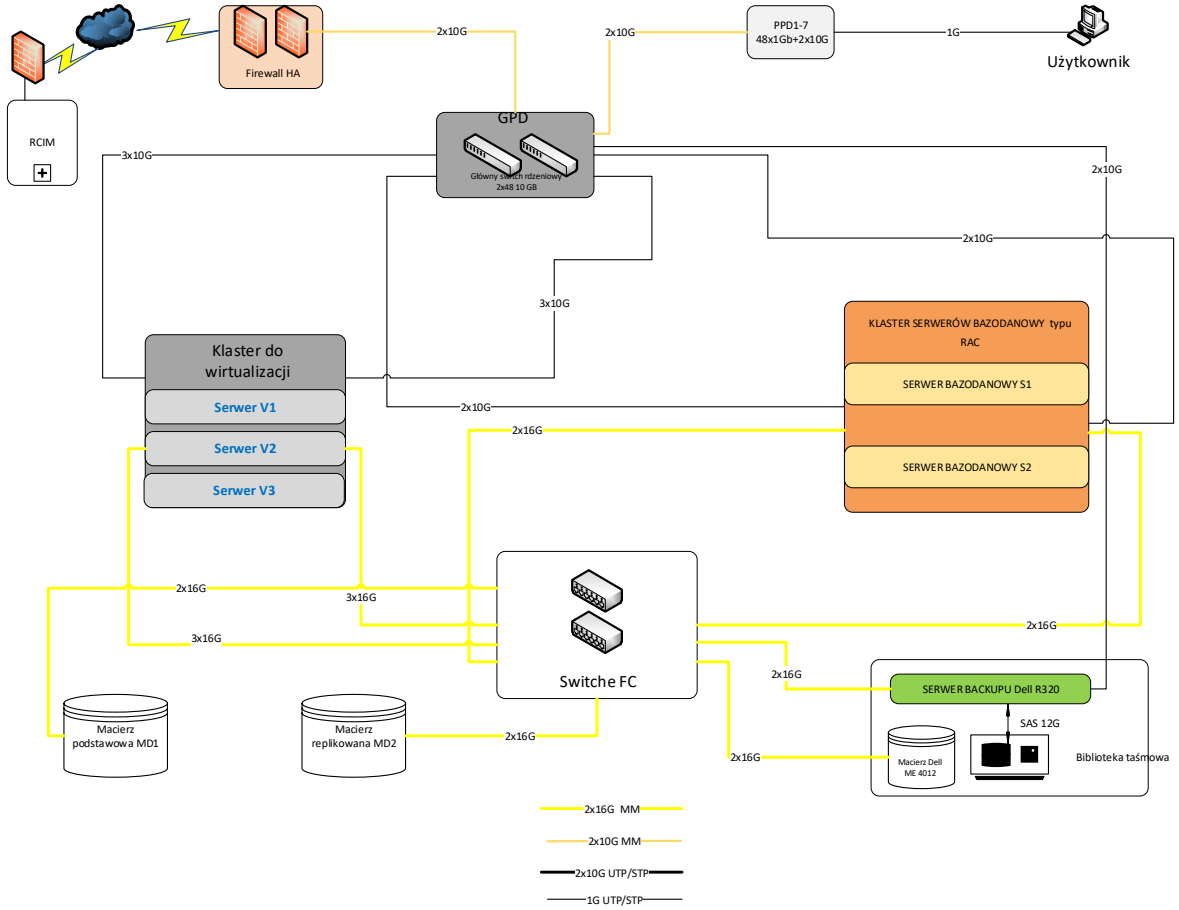


Rys. Schemat połączeń sieci SAN i LAN w obrębie środowiska wirtualnego.

6.4.5. Modernizacja środowiska backupu i archiwizacji danych

System backupu będzie składał się z następujących komponentów:

- Istniejący serwer backupu Dell R320 połączony do sieci SAN 2x16G i LAN 2x10G rozbudowany dodatkowo o:
  - kartę do serwera FC 2x16G,
  - kartę do LAN 2x10G;
- Istniejąca macierz wewnętrzna serwera Dell ME 4012 doposażona w:
  - dodatkową kartę FC 2x16G
- Nowa biblioteka taśmowa z napędem obsługującym standard LTO8;
- Nowe oprogramowanie do backupu z licencją do backupu klastra wirtualizacyjnego i klastra bazodanowego zainstalowane na serwerze backupu Dell R320.



Rys. Schemat połączeń systemu backupu.

6.4.6. Modernizacja systemu bezpieczeństwa

Dla potrzeb spełnienia wymogów bezpieczeństwa sieci wewnętrznej jak i świadczenia e-usług planuje się wdrożenie rozwiązań HA w tym obszarze poprzez zakup 2 urządzeń typu UTM. Urządzenie UTM pracujące w układzie High Availability, dają możliwość pełnego zabezpieczenia sieci, nawet w przypadku awarii sprzętowej jednego urządzenia.

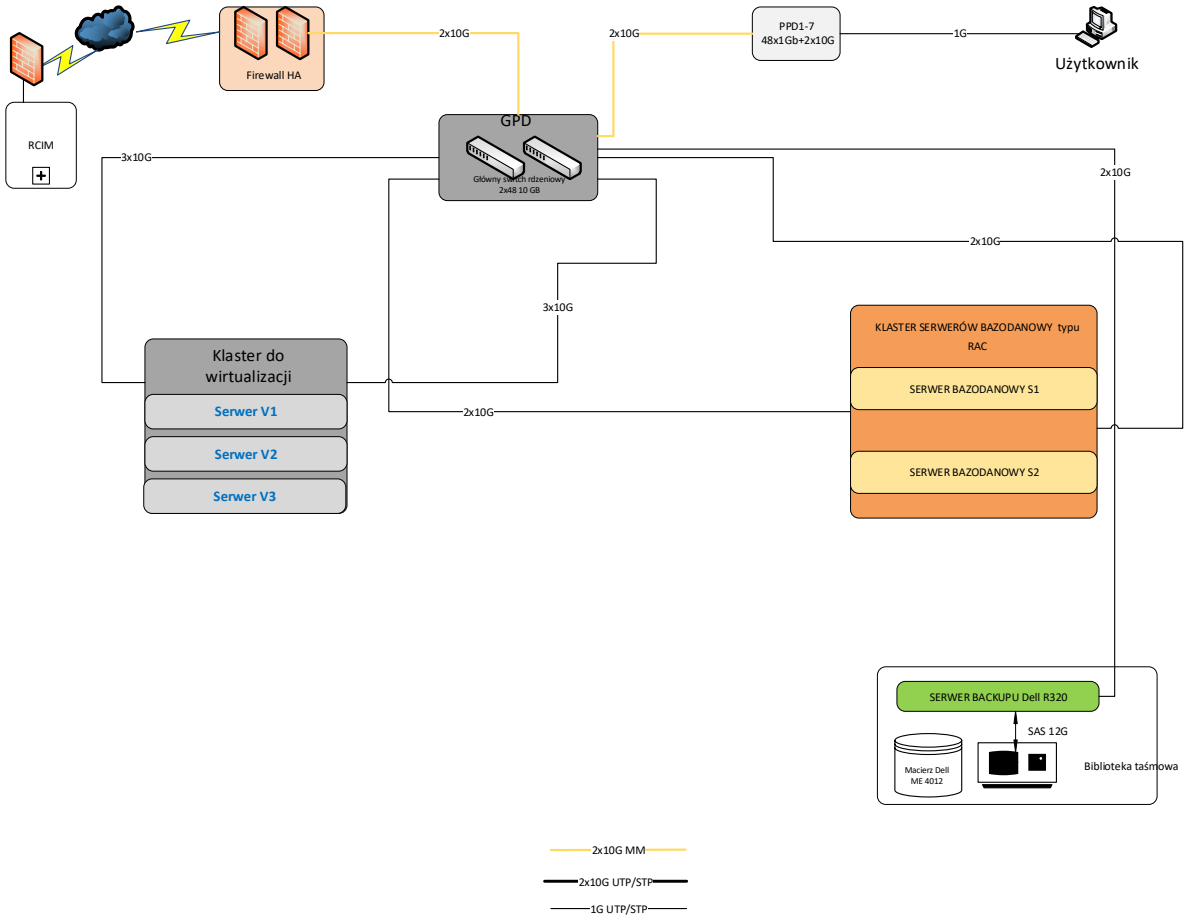
Wymogi w zakresie funkcjonalnym i parametryzacyjnym dla urządzenia/urządzeń brzegowych umożliwiające integrację z RCIM i zbudowanie szyfrowanych kanałów VPN:

- Adres IP: tak, IPv4, publiczny i stały
- Obsługa i nieblokowanie protokołu IPSec: tak, przez urządzenie brzegowe, urządzenia pośrednie i operatora
- Typ połączenia: sieć-sieć (site-to-site, S2S)
- Obsługa NAT: tak, statyczny punk-punkt
- IPSec – faza pierwsza
  - Protokół IKEv2
  - Algorytm szyfrowania AES-256
  - Algorytm haszujący SHA-1
  - Uwierzytelnianie certyfikat X.509 v1 (RFC1422)
  - Grupa algorytmu Diffie-Hellman 5 (1536 bitów)
  - Perfect Forward Secrecy (PFS) tak
  - Czas życia 86400 sekund, bez limitu ilości danych
- IPSec - faza druga

  - Algorytm szyfrowania AES-256
  - Uwierzytelnianie SHA-1
  - Perfect Forward Secrecy (PFS) grupa 5 (1536 bitów)
  - Czas życia SA 3600 sekund, 4608000 kilobajtów
- Algorytm szyfrowania AES-256
- Uwierzytelnianie SHA-1
- Perfect Forward Secrecy (PFS) grupa 5 (1536 bitów)
- Czas życia SA 3600 sekund, 4608000 kilobajtów
- Obsługa standardów RFC6071 (IPSec) RFC1422 (X.509 v1) RFC5280, RFC4945 (X.509 v3 z rozszerzeniami) RFC7468 (PEM)

Urządzenie terminujące ruch VPN w jednostce medycznej powinno posiadać co najmniej 3 interfejsy:
- interfejs światłowodowy (światłowód jednomodowy) działający z prędkością 1Gb/s,
- interfejs światłowodowy pozwalający na podłączenie łącza zapasowego,
- interfejs do dołączenia sieci lokalnej jednostki medycznej,
- Wydajność urządzenia terminującego ruch VPN w jednostce medycznej w zakresie szyfrowania ruchu IPSec nie powinna być mniejsza niż 1 Gb/s.

Zestaw urządzeń typu UTM pracujący w klastrze HA 2xUTM z pakietem usług: Stateful Inspection Firewall, Intrusion Prevention System (IDS/IPS, Virtual Private Networks (IPSec VPN, SSL VPN, PPTP), Autoryzacja użytkowników (LDAP, AD), Ochrona antywirusowa, Ochrona przed spamem, Filtr URL, SSL Proxy, Raportowanie.



Rys. Schemat umiejscowienia Urządzeń UTM (firewall).

6.5. Pakiet / Zadanie nr 5. System badań obrazowych – odkładanie do EDM.

SPZOZ w Sanoku planuje wdrożyć rozwiązanie umożliwiające udostępnianie obrazów diagnostycznych wraz z opisami zarówno w celach konsultacyjnych (np. podmiotom leczniczym) jak i pacjentom w celu łatwego i szybkiego dostępu do dokumentacji medycznej. System powinien być zintegrowany z RIS oraz z archiwum PACS Zamawiającego celem udostępniania i zarządzania zbiorem danych przez dedykowany portal internetowy, zgodny z wymaganiami WCAG 2.1.

Wymagane jest aby system umożliwiał przeglądanie udostępnionych badań obrazowych online w formacie DICOM przez wbudowane narzędzie oraz posiadał funkcję komunikacji z pacjentem.

Udostępniana dokumentacja musi zostać podpisana za pomocą kwalifikowanego podpisu elektronicznego lub certyfikatu ZUS. Wobec powyższego planowane rozwiązanie powinno posiadać narzędzie (moduł) do dokonywania autoryzacji przez lekarzy opisujących. Jeśli zaoferowane rozwiązanie nie będzie posiadać stosownego narzędzia do powyższego celu Zamawiający dopuszcza zaimplementowanie takiej funkcjonalności w oprogramowaniu już posiadanym.

W celu zapewnienia bezpieczeństwa Wykonawca dokona migracji i uruchomienia obecnie wykorzystywanych systemów PACS/RIS na maszynę sprzętową wskazaną przez Zamawiającego.

Wymagania minimalne dostarczonego oprogramowania znajdują się w w rozdziale II, punkt 5. Termin wykonania pakietu / zadania to 90 dni od wykonania pakietu / zadania nr 4.

6.6. Pakiet / Zadanie nr 6. Dostarczenie i uruchomienie modułów HIS, systemu autoryzacji wyników badań laboratoryjnych oraz e-Usług.

Zamawiający dopuszcza wykonanie pakietu / zadania tylko poprzez modernizację/rozbudowę obecnie posiadanego systemu informatycznego oraz integrację z nim nowo dostarczonych funkcjonalności, modułów i usług.

Wymagania minimalne dostarczonego oprogramowania znajdują się w w rozdziale II, punkt 6. Termin wykonania pakietu / zadania to 90 dni od wykonania pakietu / zadania nr 4.

6.6.1. Oprogramowanie dziedzinowe

Zestawienie posiadanych licencji oprogramowania dziedzinowego:

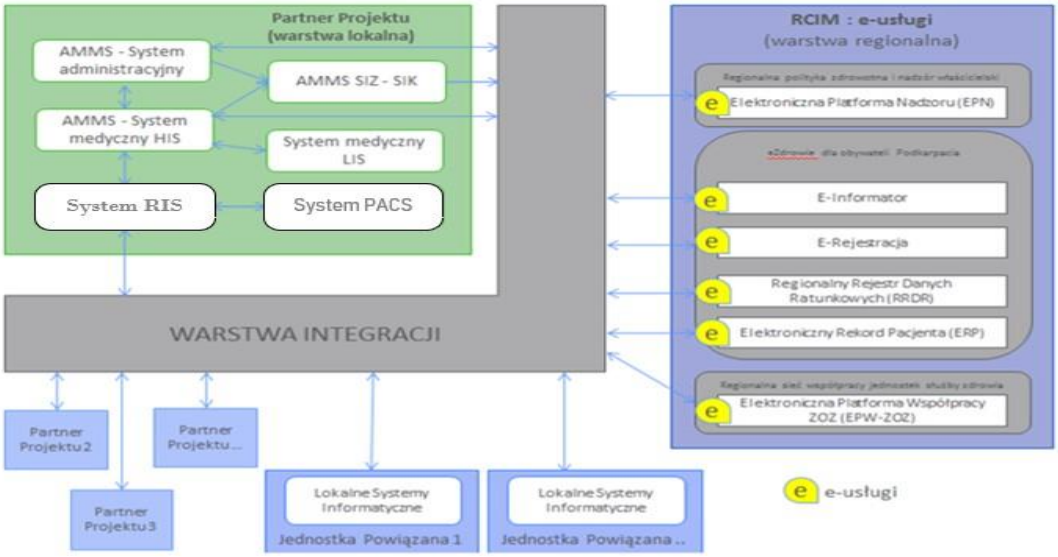
L.p.	Nazwa modułu	Licencja	Ilość
1	Finanse-Księgowość	USER	6
2	Koszty	USER	2
3	Rejestr sprzedaży	USER	3
4	Kadry	USER	4
5	Płace	USER	4
6	Ewidencja Czasu Pracy (Grafik)	USER	2

7	Gospodarka Magazynowo-Materiałowa	USER	4
8	Środki Trwałe	USER	1
9	Wycena Kosztów Normatywnych Świadczeń	USER	1
10	Kasa	USER	1
11	Rejestr Zakupów	USER	1
12	Kalkulacja Kosztów Leczenia	USER	1
13	Budżetowanie wraz z wariantami budżetowymi dla OPK	USER	1
14	Wyposażenie	USER	1
15	AMMS Ruch Chorych (Izba Przyjęć, Oddziały, Statystyka Medyczna, Zlecenia)	OPEN	1
16	AMMS – Rejestracja, Gabinety, Statystyka Medyczna, Zlecenia	OPEN	1
17	AMMS – Gabinet Zabiegowy	USER	8
18	Zarządzanie Dokumentacją Medyczną	USER	2
19	AMMS – Punkt Pobrań	USER	5
20	Laboratorium	OPEN	1
21	AMMS – Pracownia Diagnostyczna	USER	5
22	Formularzowa Dokumentacja Medyczna – Edytor Formularzy	OPEN	1
23	AMMS – Zakażenia Szpitalne	USER	1
24	AMMS – Rehabilitacja	USER	4
25	AMMS – Blok Operacyjny	USER	7
26	AMMS – Apteka	USER	7
27	AMMS – Apteczka Oddziałowa	OPEN	1
28	e-Rejestracja, e-Wiadomości, e-Dokumentacja, e-Wywiad, e-Świadczenia	OPEN	1
29	WDSZ – RIS głęboka	EVENT	1
30	WDSZ – System regionalny	EVENT	1
31	Repozytorium Elektronicznej Dokumentacji Medycznej	OPEN	1
32	SIZ2 – pakiet Finanse i Księgowość	EVENT	1
33	TOPSOR - interfejs integracyjny z systemu AMMS	EVENT	1
34	Zdarzenia Medyczne	OPEN	1
35	Bank krwi	USER	1

36	AMMS - Gabinet Medycyny Pracy	USER	2
37	AMMS - Komercja	USER	1

6.6.2. Integracja systemu HIS z e-usługami dostępnymi w ramach Podkarpackiego Systemu Informacji Medycznej (PSIM)

PSIM (Podkarpacki System Informacji Medycznej) jest rozwiązaniem regionalnym mającym na celu gromadzenie, analizę i udostępnianie zasobów cyfrowych zawierających informacje o udzielonych lub zaplanowanych w placówkach służby zdrowia świadczeniach opieki zdrowotnej. System usytuowany jest w dwóch warstwach: lokalnej (w jednostkach służby zdrowia) i regionalnej (RCIM), gdzie znajdują się usługi umożliwiające integrację jednostek warstwy lokalnej. W warstwie regionalnej znajdują się również moduły analityczne i administracyjne oraz usługi dostępne dla pacjentów.



Rys. Obecna architektura systemu lokalnego SPZOZ Sanok i RCIM w ramach PSIM.

Cała komunikacja funkcjonalna (aplikacyjna) pomiędzy warstwą regionalna (RCIM) a warstwą lokalną jednostki służby zdrowia, realizowana jest za pośrednictwem technicznych komponentów: Brokera RCIM i Adaptera ZOZ. Wszystkie wywołania przez warstwę regionalną usług realizowanych przez warstwę lokalną (systemy ZOZ), jak i wywołania przez systemy ZOZ usług udostępnionych przez warstwę regionalną, są szyfrowane. Komunikaty z danymi usługi są szyfrowane po stronie warstwy wysyłającej i odszyfrowywane po stronie warstwy odbierającej. Dotyczy to, odpowiednio, komunikatów z danymi wejściowymi do usługi oraz komunikatów z rezultatem działania usługi (dane wyjściowe).

6.7. Dostawa i instalacja produktów w ramach pakietów / zadań – zestawienie ilościowe.

Rozdz. / Punkt	Nazwa	Jedn. miary	Ilość
Pakiet / Zadanie nr 1			
II / 1.2.1	Szafa serwerowa	Szt.	1
Pakiet / Zadanie nr 2			
II / 2.2.1	Klimatyzatory	Szt.	1
Pakiet / Zadanie nr 3			
II / 3.2.1	Modernizacja UPS	Szt.	1
Pakiet / Zadanie nr 4			
II / 4.2.1	Serwer bazodanowy dwuprocesorowy S1, S2	Szt.	2
II / 4.2.2	Komercyjny silnik bazy danych	Szt.	4
II / 4.2.3	Serwery V1, V2, V3 do klastra wirtualizacyjnego	Szt.	3
II / 4.2.4	Oprogramowanie do wirtualizacji	Szt.	1
II / 4.2.5	Komercyjne systemy operacyjne pracujące w klastrze wirtualizacyjnym	Szt.	2
II / 4.2.6	Dodatkowe licencje na 2 x core	Szt.	56
II / 4.2.7	System licencji dostępowych CAL	Szt.	500
II / 4.2.8	Macierz produkcyjna główna	Szt.	1
II / 4.2.9	Macierz do replikacji	Szt.	1
II / 4.2.10	Switch FC	Szt.	2
II / 4.2.11	Dodatkowa karta do serwera istniejącego backupu	Szt.	1
II / 4.2.12	Dodatkowa karta do LAN	Szt.	1
II / 4.2.13	Dodatkowa karta SAS HBA z kablem	Szt.	1
II / 4.2.14	Biblioteka taśmowa	Szt.	1
II / 4.2.15	Oprogramowanie do backupu środowiska wirtualnego i bazodanowego	Szt.	3
II / 4.2.16	Urządzenie UTM pracujące w klastrze HA	Szt.	1
II / 4.2.17	Urządzenie do HA	Szt.	1
II / 4.2.18	Switch rdzeniowy	Szt.	2
II / 4.2.19	Moduły do switchy rdzeniowych	Szt.	20
II / 4.2.20	Switch do punktów dystrybucyjnych	Szt.	7

II / 4.2.21	Moduły do switchy dystrybucyjnych dla SM	Szt.	20
Pakiet / Zadanie nr 5			
II / 5.2.1	System badań obrazowych – odkładanie do EDM	Szt.	1
Pakiet / Zadanie nr 6			
II / 6.2.1	Licencje (moduły) do systemu HIS	Kpl.	1
II / 6.2.2	System autoryzacji wyników badań laboratoryjnych z EDM w zakresie podpisu elektronicznego	Kpl.	1
II / 6.2.3.2	RREDM – Regionalne Repozytorium EDM -udostępnianie dodatkowych e-dokumentów na platformę regionalną wytworzonych w systemie HIS	Szt.	1
II / 6.2.3.3	e-Informacja – modernizacja i rozszerzenie e-usługi w integracji	Szt.	1
II / 6.2.3.4	e-Rejestracja – modernizacja i rozszerzenie e-usługi w zakresie integracji z IKP na platformie P1	Szt.	1

Rozdział II
Szczegółowy opis pakietów / zadań

1. Pakiet / Zadanie nr 1. Dostarczenie i montaż szafy rack.

1.1. Wymagania ogólne i opis rozwiązania

- Wykonawca zobowiązany jest dostarczyć i zamontować urządzenie w miejscu wskazanym przez Zamawiającego.
- Wykonawca dokona montażu listew zasilających, panelu wentylacyjnego oraz organizerów kablowych.
- Wykonawca podłączy koryta kablowe 42U do pionowej organizacji kabli w szafie oraz koryto techniczne.

1.2. Specyfikacja szczegółowa

1.2.1. Szafa serwerowa – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymiary	800x1000mm, 42U
Nośność	1000 kg
Rodzaj drzwi przednich	Perforowane
Rodzaj drzwi tylnych	Perforowane

Kąt otwarcia drzwi	180°
Cokół	100 mm z przepustem szczotkowym w tylnej ścianie
Podstawa	Wyposażona w zestaw filtracyjny z przepustem szczotkowym do wprowadzenia kabli, nóżki poziomujące
Prowadnice	Zestaw dwóch prowadnic pionowych 42U z pokrywą i systemem zatrzaskowym oraz techniczne koryto kablowe poziome do doprowadzenia przewodów do szafy o długości 2 m
Belki nośne 19”	Wykonane z profili o grubości 2 mm z numeracją jednostek użytkowych oraz płynną regulacją ustawienia głębokości
Uziemienie	Zestaw linek uziemiających prowadzących do każdego elementu szafy
Kolor	Czarny
Materiał	Stal
Wyposażenie dodatkowe	• Listwy dystrybucji zasilania do montażu w szafie rack – 2 sztuki • Panel wentylacyjny poziomy z termostatem (min. 4 wentylatory) • Organizer kabli – 3 sztuki

2. Pakiet / Zadanie nr 2. Dostarczenie i montaż klimatyzatora.

2.1. Wymagania ogólne i opis rozwiązania

- Wykonawca zobowiązany jest dostarczyć, zamontować i uruchomić urządzenie w miejscu wskazanym przez Zamawiającego.
- Wykonawca dokona montażu jednostek wewnętrznej i zewnętrznej.
- Wykonawca wykona otwory na przewody elektryczne, freonowe i instalację odprowadzenia skroplin. Wszystkie przewody na ścianie muszą być umieszczone w korytach.
- Wykonawca dokona próby szczelności, odpowietrzenia i napełnienia układu czynnikiem chłodniczym.

2.2. Specyfikacja szczegółowa

2.2.1. Klimatyzator – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Podstawowe parametry techniczne	• Rodzaj: ścienny • Moc chłodnicza w przedziale (kW): min 5 kW • Obsługiwana powierzchnia: min. 40 m^2 • Technologia inwerterowa: tak
Dodatkowe wymagania	• Przystosowany do pracy 24 godziny na 7 dni w tygodniu. • Jednostka zewnętrzna: praca w trybie chłodzenia nawet przy temperaturze zewnętrznej minus 15°C • Wysokowydajny silnik wentylatora jednostki zewnętrznej na prąd stały zapewniający optymalne ciśnienie kondensacji (współpraca z czujnikiem temperatury orurowania jednostki zewnętrznej) • Opcje interfejsu do obsługi serwerowni

	• Interfejs współpracuje z lokalną siecią WiFi z funkcjami zaawansowanymi dla serwerowni: · Włączanie/wyłączanie, ustawienia temperatury · Automatyczna wiadomość mailowa na wypadek awarii · Wyświetlanie temperatury pomieszczenia w trybie on-line oprogramowania · Możliwość sterowania przez odpowiednie aplikacje OS Android oraz Internetu
Instalacja i konfiguracja	Montaż i uruchomienie klimatyzatora we wskazanym miejscu, ustawienie parametrów pracy

3. Pakiet / Zadanie nr 3. Modernizacja zasilacza awaryjnego UPS.

3.1. Wymagania ogólne i opis rozwiązania

- Wykonawca zobowiązany jest dostarczyć i zamontować 36 sztuk baterii w urządzeniu Eaton 9355-20-N-MBS.
- Wykonawca dokona utylizacji zużytych baterii znajdujących się w urządzeniu oraz przekaże Zamawiającemu Kartę Przekazania Odpadu potwierdzającą przeprowadzoną utylizację.
- Wymaga się przeprowadzenia diagnostyki oraz regulacji, pomiarów napięcia baterii, pomiarów prądów ładowania, sprawdzenia parametrów wejściowych i wyjściowych urządzenia oraz przeprowadzenia testów działania UPS. Po wykonanych pracach Wykonawca wystawi stosowne protokoły z pomiarów.
- Wykonawca zorganizuje prace tak, aby zminimalizować ich wpływ na ciągłość funkcjonowania działalności systemów informatycznych Zamawiającego.

3.2. Specyfikacja szczegółowa

3.2.1. Modernizacja zasilacza awaryjnego UPS – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Urządzenie i zakres modernizacji	Wymiana 36 sztuk baterii w UPS Eaton typ 9355-20-N-MBS
Typ baterii	Baterie bezobsługowe VRLA – 12V, 36Ah
Metoda ładowania	Technologia ABM lub ładowanie konserwacyjne
Kompensacja temperatury	Opcja
Nominalne napięcie baterii (ołowiowo-kwasowych)	432 V (36 x 12V, 216 ogniw)
Prąd ładowania	6A x maks. 25A
Gwarancja	Gwarancja na baterie: min. 24 miesiące

4. Pakiet / Zadanie nr 4. Dostarczenie pozostałego sprzętu i oprogramowania wraz z ich pełną konfiguracją lokalną i uruchomieniem oraz modernizacją środowiska serwerowego.

4.1. Wymagania ogólne i opis rozwiązania

- Wykonawca zobowiązany jest dostarczyć i uruchomić kompleksową platformę Infrastruktury serwerowej (serwery, macierze wraz z niezbędnym Oprogramowaniem Narzędziowym – systemowym, bazodanowym, wirtualizacyjnym, backupowym i pozostałym oprogramowaniem) dla prawidłowego funkcjonowania Szpitalnego Systemu Informatycznego i e-usług a także dokona aktualizacji oprogramowania do najnowszych stabilnych wersji.
- Jeżeli zajdzie potrzeba, wraz z dostarczaną Infrastrukturą Serwerową, Wykonawca zobowiązany jest dostarczyć niezbędne elementy np. urządzenia i wyposażenie – kable połączeniowe, listwy zasilające do szafy rack, elementy mocujące, uznane przez Wykonawcę za niezbędne i umożliwiające prawidłowe działanie całego Systemu. Dostarczona Infrastruktura Serwerowa musi zapewniać bezproblemową pracę po podłączeniu jej do sieci informatycznej (Systemu Komunikacyjnego) Zamawiającego.
- Wykonawca jest zobowiązany dokonać montażu dostarczonej Infrastruktury Serwerowej oraz oprogramowania w miejscach wskazanych przez Zamawiającego.
- Wszystkie elementy Infrastruktury serwerowej powinny zostać zamontowane w szafach rack w sposób umożliwiający ich prawidłową wentylację.
- Szczegóły dotyczące instalacji i uruchomienia Infrastruktury serwerowej zostaną ustalone w trakcie Analizy Przedwdrożeniowej.
- W zakresie części serwerowej w ramach postępowania wymagane jest wykonanie następujących usług:
  - dostarczanie infrastruktury:
    - zestawienie dostarczanych urządzeń,
    - propozycję rozmieszczenia elementów w szafach rack,
  - instalacja, montaż i uruchomienie serwerów wirtualizacyjnych i serwera bazodanowego:
    - montaż serwerów w szafach rack,
    - podłączenie serwera do sieci LAN i/lub SAN,
    - podłączenie serwera do zasilania,
    - inicjalne uruchomienie serwera,
    - testy działania serwera oraz weryfikacja parametrów,
  - instalacja, montaż i uruchomienie infrastruktury backupowej:
    - montaż urządzeń w szafie rack,
    - podłączenie urządzeń do sieci LAN i/lub SAN,
    - podłączenie urządzeń do zasilania,
    - podłączenie biblioteki taśmowej do serwera backupu/systemu pamięci masowej,
    - aktualizacja oprogramowania do najnowszej stabilnej wersji,
    - inicjalne uruchomienie urządzeń,
    - testy działania oraz weryfikacja parametrów,
  - instalacja, montaż i uruchomienie macierzy dyskowych:
    - montaż macierzy w szafie rack,
    - podłączenie macierzy do sieci LAN i/lub SAN,
    - inicjalne uruchomienie macierzy,

  - testy działania macierzy oraz weryfikacja parametrów,
- konfiguracja macierzy dyskowych:
  - przygotowanie planu rozbudowy tj.: zestawienie stosowanej nomenklatury; zestawienie serwerów, które będą korzystać z wystawianych zasobów; przygotowanie szczegółowej koncepcji konfiguracji dysków macierzy odzwierciedlającej potrzeby biznesowe; zestawienie zakupionego oprogramowania; propozycja testów odbiorczych,
- implementacja zgodna z projektem:
  - instalacja sprzętowa,
  - aktywacja zakupionego oprogramowania,
  - konfiguracja replikacji synchronicznej,
  - implementacja zaakceptowanej konfiguracji logicznej macierzy,
- testy odbiorcze:
  - definicje testów odbiorczych,
  - zestawienie stosowanej nomenklatury,
  - weryfikację zgodności z planem wdrożenia,
  - przeprowadzenie testów potwierdzających poprawność instalacji macierzy,
- przygotowanie dokumentacji powykonawczej:
  - zestawienie stosowanej nomenklatury,
  - zestawienie serwerów korzystających z wystawianych zasobów,
  - zestawienie konfiguracji dysków macierzy,
  - zestawienie mapowania udostępnionych zasobów,
  - zestawienie zakupionego i aktywowanego oprogramowania,
- instalacja oprogramowania wirtualizacyjnego i backupowego:
  - inwentaryzacja stanu obecnego tj.: zestawienie nazewnictwa poszczególnych elementów istniejącego systemu; zestawienie zainstalowanych łat systemu operacyjnego; zestawienie zainstalowanych wersji oprogramowania,
  - przygotowanie projektu technicznego tj.: zestawienie stosowanej nomenklatury; rysunki logicznej struktury systemu; propozycję nazewnictwa poszczególnych elementów systemu wirtualizacji i backupu; zestawienie wymaganych łat systemu operacyjnego (ang. Patch Management); zestawienie wymaganych wersji oprogramowania; propozycje konfiguracji systemu wirtualizacji i backupu,
  - implementacja zgodna z projektem tj.: Instalacja oprogramowania wirtualizacyjnego i backupowego; konfiguracja oprogramowania wirtualizacyjnego i backupowego; aktywacja dostarczonego oprogramowania,
  - przygotowanie dokumentacji powykonawczej, która powinna zawierać: zestawienie stosowanej nomenklatury; rysunki logicznej struktury systemu wirtualizacji i backupu; zestawienie nazewnictwa poszczególnych elementów systemu; zestawienie konfiguracji systemu wirtualizacji; zestawienie zainstalowanych łat systemu operacyjnego (ang. Patch Management); zestawienie wersji zainstalowanego oprogramowania.
- Po zakończonym montażu, instalacji i konfiguracji Wykonawca przekaże Zamawiającemu wszystkie hasła dostępowe do kont „super użytkowników” oraz dokumentację do wszystkich oferowanych urządzeń, oprogramowania narzędziowego (m.in. systemowego, bazodanowego, wirtualizacyjnego, backupowego) wraz z dokumentami potwierdzającymi nabycia dla Zamawiającego licencji oraz nośnikami danych zawierającymi zainstalowane oprogramowanie (o ile dostarcza je producent). Wykonawca wykona również instruktaże użytkowe dla wskazanych przez Zamawiającego administratorów, z zakresu konfiguracji, obsługi i prawidłowej eksploatacji zainstalowanego sprzętu.

- Sprzęt musi pochodzić z autoryzowanego przez jego producenta kanału dystrybucji w UE i nie może być obciążony uprzednio nabytymi prawami podmiotów trzecich (subdystrybucja, niezależni brokerzy) oraz musi być przeznaczony do sprzedaży na rynku polskim.
- Wszystkie urządzenia muszą być fabrycznie nowe, wyprodukowane po 1 stycznia 2022 r.

W ramach wdrożenia środowiska wirtualnego odpornego na awarię Zamawiający wymaga rozwiązania opartego o klaster wirtualizacyjny dla systemów aplikacyjnych oraz serwerów bazodanowych podłączonych do macierzy dyskowych poprzez połączenie bezpośrednie sieci SAN FC16GB.
W zakresie systemu zabezpieczenia danych zostanie wykorzystana funkcjonalność kopii wewnętrznych macierzy oraz backup maszyn wirtualnych oraz maszyny fizycznej z bazą danych na serwer backupu. Serwer backupu podłączony zostanie poprzez połączenia 10G do przełączników rdzeniowych. W zakresie ochrony całego środowiska zostaną wykorzystane funkcjonalności oprogramowania do tworzenia kopii zapasowych zainstalowane na wydzielonym serwerze backupu (serwer Dell R320 w posiadaniu Zamawiającego). Wdrożenie przewiduje realizację archiwizacji danych z serwera backupu na bibliotekę taśm LTO. Biblioteka taśm zostanie podłączona do serwera backupu z wykorzystaniem połączenia bezpośredniego sieci SAN FC16GB.
Wszystkie serwery wchodzące w skład środowiska, zostaną podłączone do sieci LAN wykorzystując rozwiązanie gwarantujące redundancję, poprzez dwa przełączniki rdzeniowe pracujące również redundantnie. W ramach przełączników rdzeniowych zostaną wydzielone odrębne sieci VLAN zgodnie z projektem analizy przedwdrożeniowej, dopasowane do potrzeb Zamawiającego. Całe środowisko będzie chronione przed zagrożeniami z zewnątrz sieci za pomocą zintegrowanego rozwiązania bezpieczeństwa sieci, w postaci klastra niezawodnościowego, dwóch fizycznych urządzeń UTM.

Zadaniem Wykonawcy jest dostawa, montaż i konfiguracja środowiska wirtualnego odpornego na awarie, opartego o jeden klaster niezawodnościowy (aplikacyjny). Wszystkie urządzenia zostaną zamontowane we wskazanym przez Zamawiającego miejscu.

W serwerowni podstawowej znajdą się urządzenia produkcyjne, tj. serwery wirtualizacji, serwer bazy danych dwa przełączniki 10G warstwy 3, macierz dyskowa, serwer plików oraz biblioteka taśmowa. Wszystkie urządzenia zostaną podłączone do systemu zasilania awaryjnego.

Połączenia w serwerowni zostaną oparte o dostarczone przełączniki rdzeniowe z wykorzystaniem redundantnych połączeń 10G. Do przełączników sieciowych zostaną podłączone dostarczane urządzenia, również w sposób zapewniający redundancję.

Na bazie tej infrastruktury zostanie zbudowany i uruchomiony klaster niezawodnościowy dedykowany dla SSI. Miejscem przechowywania danych będzie macierz w serwerowni podstawowej, na której dodatkowo zostanie uruchomiony zostanie proces automatycznej archiwizacji danych na macierz pomocniczą. Na serwerze backupu zostanie zainstalowane i skonfigurowane oprogramowanie zapewniające backup działających serwerów wirtualnych na klastrze aplikacyjnym oraz backup baz danych i środowiska z serwera bazodanowego.

W ramach instalacji należy wykonać zawarty w powyższym opisie minimalny zakres prac:
- dostawa i montaż urządzeń w szafach rack,
- podłączenie okablowania zasilającego i sygnałowego,
- uruchomienie i konfiguracja urządzeń oraz aktualizacja firmware,

- dokonanie fizycznego przyłącza do urządzeń np. UTM, switche: rdzeniowe, FC, dystrybucyjne wykorzystując istniejące łącza światłowodowe,
- połączenie urządzeń sieciowych oraz uruchomienie komunikacji pomiędzy punktami PPD,
- konfiguracja macierzy dyskowych, utworzenie odpowiednich wolumenów,
- instalacja i konfiguracja systemów operacyjnych oraz oprogramowania wirtualizacyjnego,
- uruchomienie i konfiguracja klastra niezawodnościowego,
- uruchomienie środowiska bazodanowego,
- przygotowanie planu migracji danych z istniejących systemów dziedzinowych,
- instalacja i konfiguracja oprogramowania do backupu,
- wykonanie testów akceptacyjnych w tym backupu i odtworzenia maszyn wirtualnych i baz danych,
- konfiguracja i uruchomienie Usługi Katalogowej,
- uruchomienie na urządzeniach UTM pełnej deszyfracji,
- przeniesienie i konfiguracja istniejących systemów informatycznych Zamawiającego na nowe środowisko,
- prace konfiguracyjne i uruchomieniowe.

4.2. Specyfikacja szczegółowa

4.2.1. Serwery bazy danych S1, S2 – 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa rack o wysokości max. 1U umożliwiającą instalację min. 8 dysków 2,5” z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna	Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Dwa procesory każdy 12 rdzeni, 64 bitowe, wyposażone w minimum 18MB pamięci podręcznej, osiągające w teście wydajności PassMark CPU Mark wynik min. 25785 punktów.
RAM	Min. 256GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Health Check, Memory Page Retire
Gniazda PCIe	Minimum dwa slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane dwa interfejsy sieciowe 10/25Gb Ethernet ze złączami SFP28 Możliwość instalacji wymiennie modułów udostępniających: • dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT • dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ • cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ • cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 Dodatkowo zainstalowane:

	• dwa interfejsy FC16Gb/s.
Dyski twarde	Zainstalowane 2 x min. 300GB SSD SATA fabrycznie skonfigurowane w RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. Możliwość instalacji dwóch dysków hot-swap M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10, JBOD
Wbudowane porty	min. port USB 2.0 oraz port USB 3.0, port VGA
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Min. dwa zasilacze Hot-Plug maksymalnie 800W
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych • Możliwość wyłączenia w BIOS funkcji przycisku zasilania • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez sześciu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232 • możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy • monitorowanie zużycia dysków SSD • możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi • automatyczne zgłaszanie alertów do centrum serwisowego producenta

	• automatyczne update firmware dla wszystkich komponentów serwera • możliwość przywrócenia poprzednich wersji firmware • możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram • możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera Serwer musi posiadać funkcjonalność umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normami ISO-9001:2015 oraz ISO-14001 (lub równoważnymi). Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 (lub równoważną) lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2016, Microsoft Windows 2019 x64, Microsoft Windows 2022 x64.
Normy Środowiskowe	Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - ***Wykonawca złoży dokument potwierdzający spełnianie*** **wymogu.** Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych **w postaci oświadczenia producenta serwera** (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 (lub równoważnymi) dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr - ***Wykonawca złoży dokument potwierdzający spełnianie*** **wymogu.**
Warunki gwarancji	Min. 2 lata gwarancji producenta czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

	Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

4.2.2. Komercyjny silnik bazy danych – 4 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Oferowany motor bazy danych musi być dostępny zarówno na platformy systemów operacyjnych Windows i Linux.
2	Oferowany Motor bazy danych musi mieć możliwość rozbudowy do wersji wspierającej możliwość synchronicznej replikacji danych w dwóch niezależnych centrach danych.
3	Oferowany Motor bazy danych posiada komercyjne wsparcie producenta. Nie dopuszcza się zastosowania RBD typu open-source.
4	Oferowany Motor bazy danych ma możliwość realizacji kopii bezpieczeństwa w trakcie działania (na gorąco).
5	Oferowany Motor bazy danych generuje kopie bezpieczeństwa automatycznie (o określonej porze) i na żądanie operatora oraz umożliwia odtwarzanie bazy danych z kopii archiwalnej, w tym sprzed awarii.
6	Oferowany Motor bazy danych umożliwia eksport i import danych z bazy danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków.
7	Administrator posiada możliwość wyboru danych, które mają być monitorowane w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych, a zarządzanie nimi może odbywać się z poziomu narzędzi do zarządzania bazami danych (dopuszcza się narzędzie na poziomie motoru bazy danych).
8	Hasła użytkowników są przechowywane w bazie danych w postaci niejawnej (zaszyfrowanej).
9	Dostępność oprogramowania na współczesne 64-bitowe platformy Unix (HP-UX dla procesorów PA-RISC i Itanium, Solaris dla procesorów SPARC i Intel/AMD, IBM AIX), Intel/AMD Linux 32-bit i 64-bit, MS Windows 32-bit i 64-bit. Identyczna funkcjonalność serwera bazy danych na ww. platformach.
10	Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych.
11	Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego.
12	Przetwarzanie z zachowaniem spójności i maksymalnego możliwego stopnia współbieżności. Modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jednocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych.
13	Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana.

14	Wsparcie dla wielu ustawień narodowych i wielu zestawów znaków (włącznie z Unicode).
15	Możliwość migracji zestawu znaków bazy danych do Unicode.
16	Możliwość redefiniowania przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych.
17	Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych.
18	Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych.
19	Wsparcie protokołu XA
20	Wsparcie standardu JDBC 3.0
21	Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym
22	Motor bazy danych powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL.
23	Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).
24	Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu.
25	Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).
26	Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej)
27	Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views).
28	W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek.
29	Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru użytkowników założonego w bazie danych.
30	Baza danych powinna umożliwiać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań.

31	Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych.
32	Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServe itd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online (hot backup).
33	Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych.
34	W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników.
35	Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych.
36	Motor bazy danych na poziomie wskazanego numeru wersji wydania musi zapewnić wbudowany, własny mechanizm umożliwiający uruchomienia środowiska w konfiguracji klastrowej wykorzystującej dwa węzły jako podstawę architektury rozwiązania.
37	Motor bazy danych musi oferować wbudowane rozwiązanie pozwalające na przechowywanie, analizę i wizualizację danych geolokalizacyjnych.
38	Motor bazy danych musi oferować wbudowane rozwiązanie pozwalające na analizę powiązań, relacji między danymi wraz z możliwością wizualizacji tych powiązań i przedstawienia ich wraz z relacjami w postaci graficznej.
39	Motor bazy danych musi oferować wbudowane rozwiązanie pozwalające na wykorzystanie zaawansowanych mechanizmów statystycznych, modeli danych, funkcjonalności wartościującej, celem tworzenia analiz, modelowania i predykcji danych przechowywanych w silniku bazy.
40	Licencja bez ograniczeń z zapewnionym min. 12 miesięczną gwarancją i wsparciem przez producenta silnika bazy danych.
41	Licencje motoru bazy danych nie mogą posiadać ograniczenia do ilości użytkowników ani konkretnych systemów dziedzinowych.
42	Licencje motoru bazy danych muszą być dostarczone w ilości 4 sztuk.
43	Licencja motoru bazy danych nie może posiadać ograniczenia co do wielkości przechowywanych danych oraz nie może powodować dodatkowych opłat w przypadku przyrostu danych.

4.2.3. Serwery V1, V2, V3 do klastra wirtualizacyjnego – 3 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa rack o wysokości max. 1U umożliwiającą instalację min. 8 dysków 2,5" z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.
Płyta główna	Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Dwa procesory każdy 12 rdzeni, 64 bitowe, wyposażone w minimum 18MB pamięci podręcznej, osiągające w teście wydajności PassMark CPU Mark wynik min. 25785 punktów.
RAM	Min. 256GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Health Check, Memory Page Retire
Gniazda PCIe	Minimum dwa slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane dwa interfejsy sieciowe 10/25Gb Ethernet ze złączami SFP28 Możliwość instalacji wymiennie modułów udostępniających: • dwa interfejsy sieciowe 10Gb Ethernet w standardzie BaseT • dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ • cztery interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ • cztery interfejsy sieciowe 1Gb Ethernet w standardzie BaseT • cztery interfejsy sieciowe 25Gb Ethernet ze złączami SFP28 Dodatkowo zainstalowane: • dwa interfejsy FC16Gb/s.
Dyski twarde	Zainstalowane 2 x min. 300GB SSD SATA fabrycznie skonfigurowane w RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażonego w nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. Możliwość instalacji dwóch dysków hot-swap M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy, możliwe konfiguracje poziomów RAID: 0, 1, 10, JBOD
Wbudowane porty	min. port USB 2.0 oraz port USB 3.0, port VGA
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Min. dwa zasilacze Hot-Plug maksymalnie 800W
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych • Możliwość wyłączenia w BIOS funkcji przycisku zasilania • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła

	• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 V3 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez sześciu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232 • możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy • monitorowanie zużycia dysków SSD • możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi • automatyczne zgłaszanie alertów do centrum serwisowego producenta • automatyczne update firmware dla wszystkich komponentów serwera • możliwość przywrócenia poprzednich wersji firmware • możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram • możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera Serwer musi posiadać funkcjonalność umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normami ISO-9001:2015 oraz ISO-14001 (lub równoważnymi). Serwer musi posiadać deklaracja CE. Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001 (lub równoważnymi) lub oświadczenie producenta o stosowaniu w fabrykach polityki zarządzania energią, która jest zgodna z obowiązującymi przepisami na terenie Unii Europejskiej. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2016, Microsoft Windows 2019 x64, Microsoft Windows 2022 x64.

Normy Środowiskowe	Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku - ***Wykonawca złoży dokument potwierdzający spełnianie* wymogu.** Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych **w postaci oświadczenia producenta serwera** (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych", pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 (lub równoważną) dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr - ***Wykonawca złoży dokument potwierdzający spełnianie* wymogu.**
Warunki gwarancji	Min. 2 lata gwarancji producenta czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Oświadczenie producenta serwera, potwierdzające, że sprzęt pochodzi z oficjalnego kanału dystrybucyjnego producenta. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia, oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji systemu.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

4.2.4. Oprogramowanie do wirtualizacji – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Licencje i wsparcie	Licencje muszą umożliwiać uruchomianie wirtualizacji (pełne wykorzystanie procesorów i pamięci operacyjnej) na minimum trzech dwuprocesorowych serwerach fizycznych, każdy z zainstalowaną pamięcią RAM 256GB oraz jednej konsoli do zarządzania całym środowiskiem. Wszystkie licencje muszą być dostarczone wraz z min. 3 letnim wsparciem.
Warstwa wirtualizacji	Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i musi charakteryzować się maksymalnym możliwym stopniem konsolidacji sprzętowej.

	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do min 1TB pamięci operacyjnej. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych do 8 procesorów wirtualnych każda z krokiem co jeden) Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 7, Windows NT, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008R2, SLES 10, RHEL 6, RHEL 5, Solaris wersja 10 dla platformy x86, Debian, CentOS 6.0, FreeBSD, Asianux, Ubuntu 10.10, SCO OpenServer, SCO Unixware.
Konsola zarządzająca	Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i usługami. Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.
Kopie migawkowe, klonowanie i pozostałe funckjonalności	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Rozwiązanie musi zapewnić ciągłą pracę usług. Usługi krytyczne biznesowo muszą działać bez przestoju, czas niedostępności innych usług nie może przekraczać kilkunastu minut. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały przełączone na inne serwery infrastruktury. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej, hostowanych systemów operacyjnych (np. wgrywania patch-y) i aplikacji tak aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany. Rozwiązanie musi zapewnić możliwość szybkiego wykonywania kopii zapasowych oraz odtwarzania usług. Proces ten nie może mieć wpływu na utylizację zasobów fizycznych infrastruktury wirtualnej. Zamawiający nie dopuszcza zastosowania rozwiązań opartych o rozwiązania opensource z powodu konieczności zapewnienia trwałości projektu oraz dostępu do aktualizacji oraz wsparcia technicznego.

4.2.5. Komercyjne systemy operacyjne pracujące w klastrze wirtualizacyjnym – 2 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Licencje na serwerowy system operacyjny
2	Licencje na serwerowy system operacyjny muszą uprawniać do zainstalowania serwerowego systemu operacyjnego 3 oferowanych serwerach fizycznych lub umożliwiać zainstalowanie dwóch instancji wirtualnych tego serwerowego systemu operacyjnego na każdym z 3 oferowanych serwerów fizycznych.
3	Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanych serwerach.
4	Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym.

	2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: i. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.

	iv. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: i. Dystrybucję certyfikatów poprzez http, ii. Konsolidację CA dla wielu lasów domeny, iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych, iii. Obsługi 4-KB sektorów dysków, iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode). 26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

4.2.6. Dodatkowe licencje na 2 x core – 56 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Dodatkowe licencje niezbędne do obsługi systemów operacyjnych z pozycji 4.2.5.
2	Dodatkowe licencje 2xcore wynikające ze sposobu licencjonowania oprogramowania systemowego z pozycji 4.2.5 (system operacyjny) dla serwerów pracujących w klastrze wirtualizacyjnym. Bieżąca pozycja jest uzupełnieniem pozycji w punkcie 4.2.5 (system operacyjny).

4.2.7. System licencji dostępowych CAL – 500 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Wymaga się aby oferowane licencje dla systemu operacyjnego umożliwiały korzystanie z zasobów dla 500 użytkowników (500 licencji dostępowych).

4.2.8. Macierz produkcyjna główna – 1 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Oferowana macierz dyskowa typu All-Flash musi być wyposażona, w co najmniej 2 kontrolery.
2	Urządzenie powinno być wyposażone w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwalność pracy i utrzymanie funkcjonalności macierzy w szczególności działania pamięci cache w przypadku awarii jednego ze źródeł zasilania.
3	Macierz musi obsługiwać co najmniej protokoły blokowe: FC i iSCSI. Macierz musi obsługiwać co najmniej protokoły plikowe: NFSv3, NFSv4, SMB 1, SMB 2, SMB 3/3.02, FTP, SFTP.
4	Urządzenie musi wspierać wirtualizację serwerową w zakresie: Vmware: VAAI, VASA, Vvols (protokoły FC, iSCSI), integracja macierzy z VMware vRealize Operations oraz Hyper-V: Offloaded Data Transfer (ODX) and Offload Copy for File.
5	Macierzy musi posiadać co najmniej 128GB RAM cache obsługującej odczyty i zapisy dostępne dla wszystkich wolumenów macierzy.
6	Macierz musi być odporna na awarię pamięci cache, w szczególności pamięci cache przeznaczonej do zapisu (ang. write cache) i zapewniać w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez nieograniczony czas.
7	Oferowane urządzenie powinno być wyposażone, w co najmniej 8 porty FC 16Gbps i 2 zarządzające 1GbE Base-T
8	Macierz dyskowa musi umożliwiać stosowanie dysków SSD.
9	Macierz musi być wyposażona w dyski posiadające podwójne interfejsy.
10	Macierz musi być wyposażona w globalne dyski zapasowe dla dysków lub posiadać zapasową przestrzeń rozproszoną na wszystkich dyskach macierzy danych w liczbie wynikającej z udokumentowanych zaleceń producenta macierzy.
11	Macierz musi umożliwiać rozbudowę on-line (bez konieczności wymiany bądź dokładania kontrolerów i zatrzymywania dostępu hostów do wolumenów znajdujących się na macierzy) do 500 napędów dyskowych w obrębie pojedynczego urządzenia (bez wykorzystywania urządzeń typu wirtualizator). Po rozbudowie musi być możliwy dostęp do każdego wolumenu z każdego kontrolera.
12	Macierz musi zostać wyposażona w przestrzeń fizyczną o wielkości minimum 23 TB, utworzonej przy pomocy dysków SSD.
13	Macierz musi posiadać funkcjonalność tworzenia lokalnych kopii migawkowych wewnętrznymi mechanizmami macierzy w technologii "redirect on write". Należy dostarczyć licencję na całą pojemność macierzy. Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji: Exchange, SQL Server, Oracle, VMware dla blokowych i plikowych datastore. Spójne kopie rozumiane jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. Oprogramowanie to musi rozpoznać na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów.

14	Macierz musi obsługiwać 256 kopii migawkowych per dysk logiczny LUN.
15	W przypadku odtworzenia danych z dowolnej kopii migawkowej, urządzenie musi pozwalać na poprawne zachowanie także wcześniejszych jak i późniejszych snapshotów, z zachowaniem możliwości kolejnego odtworzenia danych ze wszystkich istniejących (starszych i nowszych) kopii dostępnych dla danego zasobu.
16	Wraz z macierzą muszą być dostarczone licencje potrzebne do odtwarzania woluminu z kopii migawkowej.
17	Macierz musi obsługiwać lun masking, lun mapping i inicjowanie startu systemów operacyjnych. Należy dostarczyć licencje dla maksymalnej wspieranej liczby serwerów podłączonych do macierzy.
18	Macierz musi być wyposażona w funkcjonalność zarządzania poziomem usług (ang. Quality of Service) poprzez możliwość określania wartości „nie większej niż" (limit) dla następujących parametrów dostępu do dysku logicznego: • Ilość operacji na sekundę (IOPS), • Przepustowość (MB/s).
19	Macierz musi umożliwiać replikację synchroniczną i asynchroniczną danych blokowych. Wymagane jest dostarczenie licencji na pełną pojemność oferowanej macierzy.
20	Macierz musi umożliwiać replikację asynchroniczną danych plikowych. Wymagane jest dostarczenie licencji na pełną pojemność oferowanej macierzy.
21	Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.
22	Macierz powinna zapewniać mechanizm Thin Provisioning, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu lub w momencie, gdy aplikacja nie wykorzystała przydzielonej pojemności. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.
23	Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (ang. Space reclamation).
24	Macierz powinna oferować funkcjonalność podłączenia jej do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania macierzy.
25	Oferowane urządzenie i jego oprogramowanie powinno być objęte co najmniej 5-letnim wsparciem producenta sprzętu w trybie czasu reakcji następnego dnia roboczego w miejscu instalacji sprzętu. W okresie opieki wymagany jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Zamawiający zatrzymuje uszkodzone dyski.
26	Połączenia między dyskami a kontrolerami muszą być wykonane w technologii SAS 12Gbps.
27	Macierz musi obsługiwać zabezpieczenie RAID5 i RAID6.
28	Macierz musi umożliwiać replikację asynchroniczną dla danych plikowych pomiędzy dwiema macierzami. Wymagane jest dostarczenie licencji na pełną pojemność oferowanej macierzy.
29	Oferowana macierz dyskowa musi umożliwiać rozbudowę ilości portów FC 16Gbps do 8 na kontroler.
30	Macierz musi posiadać funkcję kompresji i deduplikacji danych in-line. Niezbędne jest dostarczenie licencji na całą pojemność macierzy.
31	Macierz musi umożliwiać szyfrowanie danych na dyskach. Niezbędne jest dostarczenie odpowiednich dysków i licencji na całą pojemność macierzy do zrealizowania tej funkcjonalności.

4.2.9. Macierz do replikacji – 1 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Oferowana macierz dyskowa typu All-Flash musi być wyposażona, w co najmniej 2 kontrolery.
2	Urządzenie powinno być wyposażone w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwalność pracy i utrzymanie funkcjonalności macierzy w szczególności działania pamięci cache w przypadku awarii jednego ze źródeł zasilania.
3	Macierz musi obsługiwać co najmniej protokoły blokowe: FC i iSCSI. Macierz musi obsługiwać co najmniej protokoły plikowe: NFSv3, NFSv4, SMB 1, SMB 2, SMB 3/3.02, FTP, SFTP.
4	Urządzenie musi wspierać wirtualizację serwerową w zakresie: Vmware: VAAI, VASA, Vvols (protokoły FC, iSCSI), integracja macierzy z VMware vRealize Operations oraz Hyper-V: Offloaded Data Transfer (ODX) and Offload Copy for File.
5	Macierzy musi posiadać co najmniej 128GB RAM cache obsługującej odczyty i zapisy dostępne dla wszystkich wolumenów macierzy.
6	Macierz musi być odporna na awarię pamięci cache, w szczególności pamięci cache przeznaczonej do zapisu (ang. write cache) i zapewniać w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez nieograniczony czas.
7	Oferowane urządzenie powinno być wyposażone, w co najmniej 8 porty FC 16Gbps i 2 zarządzające 1GbE Base-T
8	Macierz dyskowa musi umożliwiać stosowanie dysków SSD.
9	Macierz musi być wyposażona w dyski posiadające podwójne interfejsy.
10	Macierz musi być wyposażona w globalne dyski zapasowe dla dysków lub posiadać zapasową przestrzeń rozproszoną na wszystkich dyskach macierzy danych w liczbie wynikającej z udokumentowanych zaleceń producenta macierzy.
11	Macierz musi umożliwiać rozbudowę on-line (bez konieczności wymiany bądź dokładania kontrolerów i zatrzymywania dostępu hostów do wolumenów znajdujących się na macierzy) do 500 napędów dyskowych w obrębie pojedynczego urządzenia (bez wykorzystywania urządzeń typu wirtualizator). Po rozbudowie musi być możliwy dostęp do każdego wolumenu z każdego kontrolera.
12	Macierz musi zostać wyposażona w przestrzeń fizyczną o wielkości minimum 23 TB, utworzonej przy pomocy dysków SSD.
13	Macierz musi posiadać funkcjonalność tworzenia lokalnych kopii migawkowych wewnętrznymi mechanizmami macierzy w technologii "redirect on write". Należy dostarczyć licencję na całą pojemność macierzy. Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji: Exchange, SQL Server, Oracle, VMware dla blokowych i plikowych datastore. Spójne kopie rozumiane jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. Oprogramowanie to musi rozpoznać na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów.
14	Macierz musi obsługiwać 256 kopii migawkowych per dysk logiczny LUN.
15	W przypadku odtworzenia danych z dowolnej kopii migawkowej, urządzenie musi pozwalać na poprawne zachowanie także wcześniejszych jak i późniejszych snapshotów, z zachowaniem możliwości kolejnego odtworzenia danych ze wszystkich istniejących (starszych i nowszych) kopii dostępnych dla danego zasobu.
16	Wraz z macierzą muszą być dostarczone licencje potrzebne do odtwarzania woluminu z kopii migawkowej.

17	Macierz musi obsługiwać lun masking, lun mapping i inicjowanie startu systemów operacyjnych. Należy dostarczyć licencje dla maksymalnej wspieranej liczby serwerów podłączonych do macierzy.
18	Macierz musi być wyposażona w funkcjonalność zarządzania poziomem usług (ang. Quality of Service) poprzez możliwość określania wartości „nie większej niż" (limit) dla następujących parametrów dostępu do dysku logicznego: • Ilość operacji na sekundę (IOPS), • Przepustowość (MB/s).
19	Macierz musi umożliwiać replikację synchroniczną i asynchroniczną danych blokowych. Wymagane jest dostarczenie licencji na pełną pojemność oferowanej macierzy.
20	Macierz musi umożliwiać replikację asynchroniczną danych plikowych. Wymagane jest dostarczenie licencji na pełną pojemność oferowanej macierzy.
21	Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.
22	Macierz powinna zapewniać mechanizm Thin Provisioning, który polega na udostępnianiu większej przestrzeni logicznej niż jest to fizycznie alokowane w momencie tworzenia zasobu lub w momencie, gdy aplikacja nie wykorzystała przydzielonej pojemności. Wymagane jest dostarczenie niezbędnych licencji na całą pojemność macierzy.
23	Macierz musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (ang. Space reclamation).
24	Macierz powinna oferować funkcjonalność podłączenia jej do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania macierzy.
25	Oferowane urządzenie i jego oprogramowanie powinno być objęte co najmniej 5-letnim wsparciem producenta sprzętu w trybie czasu reakcji następnego dnia roboczego w miejscu instalacji sprzętu. W okresie opieki wymagany jest bezpłatne usuwanie awarii, bezpłatny dostęp do części zamiennych wymienianych w przypadku awarii oraz dostęp do wszystkich nowszych wersji oprogramowania. Zamawiający zatrzymuje uszkodzone dyski.
26	Połączenia między dyskami a kontrolerami muszą być wykonane w technologii SAS 12Gbps.
27	Macierz musi obsługiwać zabezpieczenie RAID5 i RAID6.
28	Macierz musi umożliwiać replikację asynchroniczną dla danych plikowych pomiędzy dwiema macierzami. Wymagane jest dostarczenie licencji na pełną pojemność oferowanej macierzy.
29	Oferowana macierz dyskowa musi umożliwiać rozbudowę ilości portów FC 16Gbps do 8 na kontroler.
30	Macierz musi posiadać funkcję kompresji i deduplikacji danych in-line. Niezbędne jest dostarczenie licencji na całą pojemność macierzy.
31	Macierz musi umożliwiać szyfrowanie danych na dyskach. Niezbędne jest dostarczenie odpowiednich dysków i licencji na całą pojemność macierzy do zrealizowania tej funkcjonalności.

4.2.10. Switch FC – 2 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Przełącznik FC musi być wykonany w technologii FC 16 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8 Gb/s z funkcją autonegocjacji prędkości.

2	Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla minimum 24 portów FC przełącznika.
3	Przełącznik musi być dostarczony wraz z minimum 24 modułami SFP FC 16 Gb/s.
4	Rodzaj obsługiwanych portów: D, E,F
5	Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w szafie 19".
6	Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking" uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.
7	Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk" oraz obsługiwać grupy połączeń „trunk" o różnych długościach.
8	Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów.
9	Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.
10	Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: • Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric, • Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP, • Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP, • Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów, • Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, • Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric, • Konta użytkowników definiowane w środowisku RADIUS lub LDAP, • Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS, • Obsługa SNMP v3.
11	Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
12	Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP+ umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km.
13	Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC, USB port.
14	Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S v1.1 (powinien zawierać agenta SMI-S zgodnego z wersją standardu v1.1).
15	Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP.
16	Maksymalny dopuszczalny pobór mocy przełącznika FC to 80W.
17	Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.
18	Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN.

19	Możliwość wymiany w trybie „na gorąco”: minimum w odniesieniu do modułów portów Fibre Channel (SFP+).
20	Wsparcie dla N_Port ID Virtualization (NPIV).
21	Gwarancja na sprzęt przynajmniej na dwa lata. Gwarancja powinna być świadczona w trybie 24x7x365, z czasem reakcji do następnego dnia roboczego od zgłoszenia.
22	Produkt musi być fabrycznie nowy i dostarczony przez autoryzowany kanał sprzedaży producenta na terenie kraju.
23	Szyny do montażu w szafie rack.

4.2.11. Dodatkowa karta do serwera istniejącego backupu – 1 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Karta kompatybilna z istniejącym serwerem Dell R320 (ST-F436LY1), Dual Port 16Gb Fibre Channel HBA, Low Profile.

4.2.12. Dodatkowa karta do LAN – 1 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Karta kompatybilna z istniejącym serwerem Dell R320 (ST-F436LY1), Dual Port (2 x SFP+, 10GbE, PCI-E)

4.2.13. Dodatkowa karta SAS HBA z kablem – 1 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Karta kompatybilna z istniejącym serwerem Dell R320 (ST-F436LY1), 12GB SAS HBA (Dual Port)

4.2.14. Biblioteka taśmowa – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa i pojemność	Wysokość maksymalnie 1U do instalacji w szafie rack. Co najmniej 9 slotów przeznaczonych na zestaw taśm.
Połączenie	Co najmniej 1 port SAS o przepustowości co najmniej 6Gb/s w standardzie umożliwiającym podłączenie serwerów.
Napęd	Wyposażony w co najmniej 1 sztukę napędów, o parametrach: • Standard LTO8, • Obudowa o wysokości max 1U, • Przepustowość co najmniej 500GB/hr, • W komplecie min. 5 taśm LTO8 oraz taśma czyszcząca, • W komplecie kabel SAS umożliwiający podłączenie biblioteki do serwera o dł. min. 2m.
Gwarancja	• Przynajmniej 2 lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.

	• Możliwość rozszerzenia wsparcia producenta o dedykowanego koordynatora koordynującego prace serwisowe, dostarczenia przez producenta miesięcznych raportów dotyczących częstotliwości występowania usterek, jakości i terminowości wykonywanych napraw, zaleceń dotyczących instalacji nowych sterowników oraz mikrokodu urządzenia. • Wszystkie naprawy gwarancyjne realizowane w miejscu instalacji. • Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu. • W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).

4.2.15. Oprogramowanie do backupu środowiska wirtualnego i bazodanowego – 3 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
2	Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time).
3	Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.
4	Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych.
5	Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn.
6	Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
7	Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
8	Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
9	Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
10	Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska.
11	Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska.
12	Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
13	Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

14	Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego.
15	Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
16	Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.
17	Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere.
18	Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.
19	System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na Vmware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich.
20	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Vmware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.
21	System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
22	System musi mieć status „Vmware Ready” i być przetestowany i certyfikowany przez Vmware.
23	System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter.
24	System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn.
25	System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz XLS.
26	System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk.
27	System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora.
28	System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów.
29	System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard).
30	System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna.
31	System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego.
32	System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta.

33	System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
34	System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
35	System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware
36	System musi mieć możliwość monitorowania instancji Vmware vCloud Director w wersji 8.x i 9.x.
37	System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na Vmware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016 oraz 2019.
38	System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
39	System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.
40	System musi mieć możliwość eksportowania raportów do formatów DOC, XLS, PDF.
41	System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.
42	System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach.
43	System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.
44	System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.
45	System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.
46	System musi mieć możliwość analizowania „przeszacowanych" wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.
47	System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.
48	System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
49	System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.
50	System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy Vmware.
51	System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).
52	System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.

53	Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.
54	Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.
55	Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE.
56	Rozwiązanie musi wspierać systemy operacyjne macOS.
57	Rozwiązanie musi wspierać następujące wersje macOS: Big Sur, Catalina.
58	Rozwiązanie musi wspierać wykonywanie kopi zapasowych następujących systemów plików: NTFS, ReFS, FAT32, ext2, ext3, ext4, ReiserFS, JFS, XFS, F2FS, Brtfs (dla kernela 3.16 i nowszych), APFS, HFS, HFS+, NILFS2.
59	Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).
60	Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster.
61	Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.
62	Rozwiązanie musi wspierać backup podłączonych dysków USB.
63	Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.
64	Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na: • Lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, • Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, • Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, • Zcentralizowanym repozytorium danych, • Bezpośrednio na zasobach Chmury.
65	Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.
66	Rozwiązanie musi wspierać kontrolę pasma sieciowego.
67	Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.
68	Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.
69	Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania blokowych kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.
70	Rozwiązanie musi wspierać skrypty wykonywane przed i po wykonaniu zadania oraz przed i po wykonaniu migawki na poziomie wolumenu.
71	Rozwiązanie musi wspierać technologię BitLocker.
72	Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.
73	Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla: • Microsoft Exchange 2010 i nowszych,

	• Microsoft Active Directory 2003 I nowszych, • Microsoft Sharepoint 2010 i nowszych, • Microsoft SQL 2005 i nowszych, • Oracle 11g i nowszych.
74	Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.
75	Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL poprzez bezpośrednie uruchomienie ich z pliku backupu.
76	Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
77	Rozwiązanie musi wspierać szyfrowanie.
78	Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.
79	Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.
80	Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.
81	Powyższa funkcjonalność ma działać w środowisku wirtualnym zbudowanym z trzech serwerów fizycznych 2 procesorowych i dwóch serwerów dwuprocesorowych.

4.2.16. Urządzenie UTM pracujące w klastrze HA – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn. zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. 3. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 4. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 5. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna

	istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. 6. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall, • Ochrony w warstwie aplikacji, • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, dysk, zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: • 12 portami Gigabit Ethernet RJ-45, • 2 gniazdami SFP+ 10 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB. 5. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 12 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.
Funkcje systemu bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Analiza ruchu szyfrowanego protokołem SSH.

	13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS), • Microsoft Azure, • Google Cloud Platform (GCP), • OpenStack, • VMware NSX.
Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2, • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM), • Obsługa protokołu Diffie-Hellman grup 19 i 20, • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE, • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site, • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego, • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth, • Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0, • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta, • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego, • Policy Based Routingu, • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

	3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,

	• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres min 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). Certyfikat ISO 9001 podmiotu serwisującego.

Konfiguracja	Wykonawca wykona prace (określone na etapie analizy przedwdrożeniowej) mające na celu przyłączenie do urządzenia UTM dwóch światłowodowych łączy internetowych oraz dokona konfiguracji urządzenia do współpracy z dwoma dostawcami ISP. Konfiguracja będzie polegała na ustawieniu „trybu równoważenia obciążenia" łączy. W przypadku awarii jednego z urządzeń UTM, jego zadania powinien przejmować drugi.

4.2.17. Urządzenie do HA – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Licencja	Dodatkowa licencja do pracy w klastrze HA.
Wymagania ogólne	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań. 3. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. 4. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. 5. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. 6. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall, • Ochrony w warstwie aplikacji, • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
Interfejsy, dysk, zasilanie	1. System realizujący funkcję Firewall musi dysponować minimum: • 12 portami Gigabit Ethernet RJ-45, • 2 gniazdami SFP+ 10 Gbps. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

	3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB. 5. System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1. W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 260 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 26 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 12 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 4 Gbps.
Funkcje systemu bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2. 12. Analiza ruchu szyfrowanego protokołem SSH. 13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. 5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu. • Amazon Web Services (AWS), • Microsoft Azure, • Google Cloud Platform (GCP), • OpenStack, • VMware NSX.

Połączenia VPN	1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2, • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode (GCM), • Obsługa protokołu Diffie-Hellman grup 19 i 20, • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE, • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site, • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego, • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth, • Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0, • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta, • Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego, • Policy Based Routingu, • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
Funkcje SD-WAN	1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.
Zarządzanie pasmem	1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
Ochrona przed atakami	1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

	4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
Kontrola aplikacji	1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
Kontrola WWW	1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. 4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

	5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
Logowanie	1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG.
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall.
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres min 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). Certyfikat ISO 9001 podmiotu serwisującego.
Konfiguracja	Wykonawca wykona prace (określone na etapie analizy przedwdrożeniowej) mające na celu przyłączenie do urządzenia UTM dwóch światłowodowych łączy internetowych oraz dokona konfiguracji urządzenia do współpracy z dwoma dostawcami ISP. Konfiguracja będzie polegała na ustawieniu „trybu równoważenia obciążenia" łączy. W przypadku awarii jednego z urządzeń UTM, jego zadania powinien przejmować drugi.

4.2.18. Switch rdzeniowy – 2 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje: • Ilość portów 24 porty SFP+ oraz 24 porty 10GBaseT niezależne • Chłodzenie od przodu do tyłu obudowy • Dwa wewnętrzne zasilacze AC • Tablica MAC min. 128K • Tablica ARP/NDP min. 8K • Bufor 56Mb • MTBF min. 133176 godzin

	• Wydajność min. 714 Mp/s • Przepustowość min. 960 Gb/s • Port USB • Port miniUSB • Port zarządzania Out-of-band • Web GUI • HTTPs • CLI • Telnet • SSH • SNMP • MIB RSPAN • Radius • TACACS+ • DiffServ • Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram • IPv4/IPv6 Multicast filtering • IGMPv3 MLDv2 Snooping • ASM & SSM • IGMPv1,v2 Querier • Auto-VoIP • Auto-iSCSI • Policy-based routing (PBR) • LLDP-MED • Spanning Tree • Green Ethernet • STP • MTP • RSTP • PV(R)STP • BPDU/STRG Root Guard • EEE (802.3az) • GVRP/GMRP • Q in Q • Private VLAN • DOT1X • MAB • Captive Portal • DHCP Snooping • Dynamic ARP • Inspection • IP Source Guard • CPU min 800 Mhz • Min 1GB RAM • Min 256MB Flash • Min ilość obsługiwanych VLAN 4K • DHCP Server min 2K rezerwacji • sFlow • Minimalna ilość przełączników w stosie: 8 • Możliwość łączenia w stos za pomocą interfejsów 10Gb/s • Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh • Non-stop forwarding (NSF) • Distributed Link Aggregation (LAGs across the stack) • Ilość interfejsów IP 128 • Double VLAN Tagging (QoQ) • PIM-DM (Multicast Routing - dense mode) • PIM-DM (IPv6) • PIM-SM (Multicast Routing - sparse mode) • PIM-SM (IPv6)

	• RIPv2 • RFC 2328 • RFC 1583 • OSPFv3 • OSPFv2 min. sąsiadów 400 • OSPFv3 min. sąsiadów 400 • OSPFv3 min. sąsiadów na interfejs 100 • UDLD • LLPF • DHCPv6 Snooping • wysyłanie alertów na email • MMRP • Ilość ACL min. 100 • Ilość reguł na listę min. 1023 na wejściu • Zasilacz z certyfikatem 80+ • CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014 • Class A, EN 61000-3-3:2013, EN 55024:2010 • VCCI : VCCI-CISPR 32:2016, Class A • RCM: AS/NZS CISPR 32:2013 Class A • FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014 • ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014 • BSMI: CNS 13438 Class A
2	• zamawiający wymaga aby przełączniki zostały uruchomione w stosie • należy dostarczyć kable krosowe miedziane w ilości 48 szt. – cat. 6. • możliwość montażu w szafie rack 19” • wysokość 1U
3	Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

4.2.19. Moduły do switchy rdzeniowych – 20 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Moduł kompatybilny z przełącznikami rdzeniowymi 10GE SR SFP+ MODULE wraz z kablem połączeniowym

4.2.20. Switch do punktów dystrybucyjnych – 7 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje: • Ilość portów 48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne • Chłodzenie od przodu do tyłu obudowy • Możliwość instalacji redundantnego zasilacza • Tablica MAC min. 16K • Tablica ARP/NDP min. 888 • Bufor 16Mb • MTBF min. 578472 godzin • Wydajność min. 130,9 Mp/s • Przepustowość min. 176 Gb/s • Port USB • Port miniUSB

	• Port zarządzania Out-of-band • Web GUI • HTTPs • CLI • Telnet • SSH • SNMP • MIB RSPAN • Radius • TACACS+ • DiffServ • Możliwość łączenia w stos za pomocą interfejsów 10Gb/s • Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh • Non-stop forwarding (NSF) • Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram • IPv4/IPv6 Multicast filtering • IGMPv3 MLDv2 Snooping • ASM & SSM • IGMPv1,v2 Querier • Auto-VoIP • Auto-iSCSI • Policy-based routing (PBR) • LLDP-MED • Spanning Tree • Green Ethernet • STP • MTP • RSTP • PV(R)STP • BPDU/STRG Root Guard • EEE (802.3az) • GVRP/GMRP • Q in Q • Private VLAN • DOT1X • MAB • Captive Portal • DHCP Snooping • Dynamic ARP • Inspection • IP Source Guard • CPU min 800 Mhz • Min 1GB RAM • Min 256MB Flash • Min ilość obsługiwanych VLAN 4K • OSPFv3 min. sąsiadów na interfejs 100 • UDLD • LLPF • DHCPv6 Snooping • wysyłanie alertów na email • MMRP • Ilość ACL min. 100 • Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu • Zasilacz z certyfikatem 80+ • CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014 • Class A, EN 61000-3-3:2013, EN 55024:2010 • VCCI : VCCI-CISPR 32:2016, Class A • RCM: AS/NZS CISPR 32:2013 Class A • FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014

	• ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014 • BSMI: CNS 13438 Class A
2	• zamawiający wymaga aby przełączniki zostały uruchomione w stosie • należy dostarczyć kable krosowe miedziane w ilości 300 szt. cat. 6 o długości 1 m • możliwość montażu w szafie rack 19” • wysokość 1U
3	Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

4.2.21. Moduły do switchy dystrybucyjnych dla SM – 20 szt.

L.p.	Charakterystyka (wymagania minimalne)
1	Moduł kompatybilny z przełącznikami rdzeniowymi 10GE SR SFP+ MODULE wraz z kablem połączeniowym

5. Pakiet / Zadanie nr 5. System badań obrazowych – odkładanie do EDM

5.1. Wymagania ogólne i opis rozwiązania

- Wykonawca dokona migracji systemów PACS/RIS na maszynę sprzętową wskazaną przez Zamawiającego.
- Wykonawca zobligowany jest do integracji systemu RIS funkcjonującym w szpitalu z modułem Elektronicznej Dokumentacji Medycznej w zakresie opisanym w parametrach poniżej.
- Wykonawca zorganizuje prace tak, aby zminimalizować ich wpływ na ciągłość funkcjonowania działalności systemów informatycznych Zamawiającego.
- Wykonawca zdefiniuje reguły udostępniania badań obrazowych oraz dokumentacji medycznej.
- Zdefiniowanie reguł dostępu na podstawie wartości zdefiniowanych atrybutów np. użytkownik autoryzujący się adresem mailowym dostępu do badań zlecanych przez tą jednostkę.
- Wykonawca skonfiguruje platformę służącą do powiadomień użytkowników poprzez SMS lub e-mail.
- Wykonawca skonfiguruje portal służący do udostępniania wyników pacjentom (podgląd obrazów, wyników badań).
- Wykonawca skonfiguruje portal służący do udostępniania wyników dla kontrahentów i do telekonsultacji (podgląd obrazów, wyników badań).
- Stworzenie wymaganych raportów i zestawień określonych przez Zamawiającego.

5.2. Specyfikacja szczegółowa

5.2.1. System badań obrazowych – odkładanie do EDM – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	• System gromadzi dane medyczne DICOM • System dostępny jest jako internetowy portal udostępniania wyników, umożliwiający wgląd online do wyników badań radiologicznych

	• System gromadzi oraz udostępnia obrazy radiologiczne wraz z opisem (jeśli dostępny) • Beneficjentem systemu jest pacjent oraz kontrahenci podmiotu wykonującego badania • System zbierania i archiwizowania danych medycznych posiada budowę modułową • System zbierania i archiwizowania danych medycznych obsługuje SSO, przechodzenie pomiędzy modułami systemu nie wymaga ponownego logowania • System zbierania i archiwizowania danych medycznych korzysta z serwera autoryzacji i autentykacji użytkowników w standardzie OAuth 2.0 • System ma możliwość wykorzystania usługi EPUAP i logowanie Profilem Zaufanym • System ma możliwość autoryzacji użytkowników poprzez platformę centralną RCIM jako dostawcę tożsamości, jeśli platforma centralna taką usługę udostępnia • Usługa autentykacji użytkowników w systemie oparta może zostać na kilku niezależnych katalogach użytkowników (użytkownicy zewnętrzni, katalog LDAP placówki szpitalnej) • Interfejs użytkownika systemu jest zrealizowany jako aplikacja WWW • Do prawidłowego działania systemu zbierania i archiwizowania danych medycznych wymagana jest zaktualizowana przeglądarka Firefox lub Google Chrome w najwyższej wersji • System zbierania i archiwizowania danych medycznych dostępny jest w polskiej i angielskiej wersji językowej • System zbierania i archiwizowania danych medycznych jest wyrobem medycznym w klasie IIb • Producent systemu posiada wdrożone systemy ISO 13485, 9001, 2700 (lub równoważne) • System spełnia zasady interoperacyjnego współdziałania na trzech poziomach: semantycznym, organizacyjnym oraz technologicznym zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2012 poz. 526, z późn. zm.) • Integracja z systemami szpitala powinna być zgodna z zasadami interoperacyjności i wykorzystywać co najmniej jeden ze standardów: HL7 v2, HL7 FHIR, HL7 CDA PIK poprzez XDS.b czy też IHE Mobile access to Health Documents (MHD) - RESTFul interface XDS on FHIR) • Internetowy portal ma zapewnić pacjentom większą dostępność usług świadczonych przez placówkę ochrony zdrowia realizującą zadania publiczne w postaci elektronicznej oraz zwiększenie efektywności tych usług • Min. 48-miesięczna gwarancja zawierająca m.in. zapewnienie poprawności działania, prawo do aktualizacji, zapewnienie wsparcia technicznego
Integracja z systemem PACS	• Oprogramowanie musi zostać zintegrowane z archiwum PACS celem udostępniania pacjentowi wyników badań obrazowych • Musi umożliwić podłączenie więcej niż jednego serwera PACS • Zasilenie systemu zbierania i archiwizowania danych medycznych jest możliwe poprzez udostępniony interfejs HL7 (v2 lub FHIR) lub standard DICOM 3.0 • W przypadku standardu HL7 FHIR dane z zewnętrznych systemów PACS pozyskiwane są za pomocą adapterów danych, umożliwiających dostęp do w/w systemów • Informowanie o nowych badaniach może odbywać się również alternatywnie poprzez komunikaty HL7 v2 i/lub komunikaty MPPS wg standardu DICOM 3.0 • Informacja o wykonanej akwizycji badania powinna się pojawić w portalu nie później niż 5 minut od zakończenia akwizycji • W systemie znajdują się kompletne dane pochodzące z systemu PACS dotyczące danych personalnych pacjenta oraz badań o określonej modalności (CT, RTG, XA, MG, RM, RF etc.) • Modyfikacja danych pacjenta w archiwum PACS musi skutkować modyfikacją danych w systemie udostępniania wyników • Zmiana przynależności serii do badania powinna skutkować zmianą w systemie udostępniania wyników
Portal udostępniania wyników jako Portal pacjenta	• Portal udostępniania wyników umożliwia podgląd obrazów oraz opisów badań radiologicznych dla pacjenta • Po wykonaniu badania radiologicznego informacja o wykonaniu badania przesyłana jest do systemu

	• System musi wysyłać powiadomienie o dostępnym badaniu do pacjenta na adres mail i/lub poprzez SMS • Wiadomość wysyłana do użytkownika zawiera link do Portalu umożliwiający dostęp do badania • System umożliwia definiowanie czasu obowiązywania wysyłanego linku do badania. Czas obowiązywania definiowany jest przez administratora systemu • Pacjent może skorzystać z logowania Profilem Zaufanym • Alternatywnie pacjent może zalogować się do systemu podając numer PESEL oraz telefon. Po weryfikacji danych w systemie placówki portal wyśle kod jednorazowego logowania • System prezentuje pacjentowi zasoby w zakresie badań obrazowych oraz Elektronicznej Dokumentacji Medycznej pacjenta • Najnowsze badania widoczne są w pierwszej kolejności • System prezentuje badania pacjenta na osi czasu lub jako listę umożliwiając łatwą nawigację do wybranej daty • System umożliwia podgląd wyniku badania radiologicznego poprzez przeglądarkę obrazów radiologicznych • System umożliwia pobranie obrazów badania radiologicznego w formie obrazu ISO lub pliku ZIP. W obu przypadkach pobierane zostaje podmiotowe badanie wraz z przeglądarką umożliwiającą podgląd badania (opcjonalnie) • W przypadku Elektronicznej Dokumentacji Medycznej system umożliwia podgląd dokumentu HL7 CDA zgodnie z wizualizacją publikowaną przez CSIOZ • System umożliwia wydruk EDM oraz pobranie dokumentu XML dla dokumentów podpisanych podpisem elektronicznym • System wyświetla powiadomienia o ostatnich aktywnościach dotyczących aktualnie zalogowanego użytkownika oraz jego dokumentów, np. uzyskanie dostępu do dokumentu, pojawienie się wyniku badania w systemie • Sposób prezentacji treści w systemie dla pacjenta powinny być zgodną z wymaganiami Web Content Accessibility Guidelines (WCAG 2.1)
Portal udostępniania wyników jako Portal Kontrahenta	• Portal udostępniania wyników umożliwia podgląd obrazów oraz opisów badań radiologicznych • Portal udostępniania wyników umożliwia podgląd EDM • Administrator systemu definiuje reguły udostępniania badań obrazowych oraz dokumentacji medycznej • Reguły udostępniania określają kto ma dostęp do jakich zasobów w ramach portalu • Dla danych obrazowych, bazując na wartościach tagów DICOM, możliwe jest zdefiniowanie reguł dostępu na podstawie wartości zdefiniowanych atrybutów, np. użytkownik autoryzujący się adresem mailowym w domenie jednostki zlecającej otrzymuje dostęp do badań zlecanych przez tą jednostkę • Dla danych z dokumentacji medycznej na podstawie wybranych atrybutów dokumentu elektronicznego możliwe jest zdefiniowanie reguł dostępu do dokumentów posiadających określoną wartość atrybutu dla wskazanych grup użytkowników • System umożliwia pobranie obrazów badania radiologicznego w formie obrazu ISO lub pliku ZIP. W obu przypadkach pobierane zostaje podmiotowe badanie wraz z przeglądarką umożliwiającą podgląd badania (opcjonalnie) • W przypadku Elektronicznej Dokumentacji Medycznej system umożliwia podgląd dokumentu HL7 CDA zgodnie z wizualizacją publikowaną przez CeZ. • System umożliwia wydruk EDM oraz pobranie dokumentu XML dla dokumentów podpisanych podpisem elektronicznym • System wyświetla powiadomienia o ostatnich aktywnościach dotyczących aktualnie zalogowanego użytkownika oraz jego dokumentów, np. uzyskanie dostępu do dokumentu, pojawienie się wyniku badania w systemie
Portal udostępniania wyników jako Portal telekonsultacji	• Portal udostępniania wyników umożliwia podgląd obrazów oraz opisów badań radiologicznych • Portal udostępniania wyników umożliwia podgląd EDM • System umożliwia udostępnienie wglądu do badania obrazowego oraz EDM innemu użytkownikowi systemu

	• Użytkownik, któremu można udostępnić dokumenty, musi zostać zweryfikowany przez administratora systemu i dodany do listy użytkowników zaufanych (katalog osób konsultujących)
	• Użytkownik systemu może złożyć wniosek/zgłoszenie do administratora z prośbą o dodanie do osób konsultujących
	• Osobie konsultującej można wybrać zakres konsultacji ze zdefiniowanej listy usług (wg standardu kodowania ICD-9) oraz dostępne formy (online, offline)
	• Określa również czas trwania konsultacji online
	• Dla użytkownika wykonującego konsultacje online w formie video rozmowy możliwe jest wprowadzenie grafiku dostępności
	• Dla użytkownika konsultanta system umożliwia zdefiniowanie zakresu możliwych do konsultowania zasobów
	• Panel zlecającego konsultacje umożliwia wyszukiwanie dokumentów do konsultacji min poprzez podanie danych pacjenta (imię, nazwisko, data urodzenia, PESEL) oraz filtr rodzaju zasobu
	• System umożliwia wytworzenie konsultacji polegającej na wskazaniu przez zlecającego konsultację zakresu dokumentów podmiotowych konsultacji oraz wyborze osoby konsultującej
	• W celu wytworzenia konsultacji konieczne jest wybranie co najmniej jednego dokumentu
	• Wytworzenie konsultacji wymaga podania przyczyny konsultacji (np. podejrzewanego rozpoznania wg kodowania ICD-10)
	• Wytworzenie konsultacji wymaga wyboru osoby konsultującej oraz formy konsultacji.
	• System udostępnia konsultacje co najmniej w formie:
	  ◦ online w formie audio/video, audio lub chat
	  ◦ offline - wysłanie żądania konsultacji ze wskazaniem oczekiwanego czasu realizacji
	• Dla konsultacji online system umożliwia wybór terminu wg harmonogramu dostępności osoby konsultującej
	• Wytworzenie i zaakceptowanie konsultacji w systemie skutkuje wysłaniem potwierdzenia konsultacji do wszystkich stron biorących w niej udział
	• Osoba konsultująca ma możliwość potwierdzenia odbycia konsultacji. To czy konsultacja wymaga potwierdzenia wprowadzane jest jako atrybut konsultacji w grafiku konsultującego
	• Panel wykonującego konsultacje wyświetla listę konsultacji w podziale na rodzaj konsultacji oraz status (wykonane, oczekujące)
	• Lista konsultacji oczekujących domyślnie jest posortowana wg priorytetu i czasu wykonania konsultacji
	• Jeśli w trakcie wykonywania konsultacji dodana zostaje konsultacja pilna, system wyświetla powiadomienie o takim zdarzeniu
	• Jeśli konsultujący otrzymuje pilną do wykonania konsultację system wysyła również powiadomienie SMS
	• Wynikiem konsultacji jest dokument elektronicznej dokumentacji medycznej, podpisany podpisem elektronicznym
	• Wynik konsultacji przechowywany jest w ramach dokumentacji medycznej pacjenta, w zależności
	• System daje możliwość dla administratora uzyskania raportów i zestawień o odbytych konsultacjach

Udostępnianie Elektronicznej Dokumentacji Medycznej	• Elektroniczna dokumentacja medyczna pacjenta udostępniana jest w formie dokumentów w formacie HL7 CDA • Rozwiązanie jest wyposażone w moduł do dokonywania autoryzacji przez lekarzy opisujących lub Wykonawca zaimplementuje narzędzie do składania podpisów elektronicznych w oprogramowaniu posiadanym przez Zamawiającego • Format dokumentów zgodny jest z wersją HL7 CDA wg Polskiej Implementacji Krajowej w wersji co najmniej 1.3.2 • Integracja systemu możliwa jest poprzez interfejs WebServices lub REST udostępniany przez producenta systemu EDM • Integracja polega na aktywnym odpytywaniu EDM przez system o nowe dokumenty lub zmiany w już pobranych dokumentach • Alternatywnie system może być powiadamiany o zdarzeniach dotyczących dokumentów przez system EDM minimum w zakresie:

	◦ utworzenia nowego dokumentu ◦ modyfikacji istniejącego dokumentu ◦ usunięcia dokumentu • Udostępniana dokumentacja może być podpisana za pomocą kwalifikowanego podpisu elektronicznego lub certyfikatem ZUS • Usługa będzie możliwa do zintegrowania z platformą regionalną województwa w ramach standardów wymiany danych HL7 CDA • Usługa zapewnia stały dostęp pacjentom do własnej dokumentacji medycznej
Moduł powiadomień użytkownika	• Platforma musi posiadać system powiadamiania min. o akcjach zachodzących na portalu, m.in. udostępnienie, dodanie opisu do badania • Powiadomienia wysyłane są do użytkowników poprzez w pełni konfigurowalny moduł powiadomień SMS/email • Moduł powiadomień współpracuje z kilkoma bramkami SMS, min. SerwerSMS, SMSApi, Clickatell • Moduł powiadomień posiada konfigurowalne szablony powiadomień. Administrator systemu korzystając z dostępnych zmiennych w wiadomości może zdefiniować treść wysyłanej wiadomości oraz kanał komunikacyjny gdzie wiadomość będzie wysyłana • Do wysyłanej wiadomości mailowej można dołączyć dowolny zestaw załączników plikowych • Możliwe jest zdefiniowanie adresata w formie adresu mail, dla którego system będzie wysyłał historię wiadomości (backup wiadomości) • Moduł powiadomień posiada graficzny interfejs administracyjny umożliwiający weryfikację poprawności wysyłki wiadomości
Integracja z systemem RIS - Autentykacja	• System przeprowadza weryfikację pacjentów za pomocą źródła danych jakim jest baza danych systemu RIS • Zalogowanie się do systemu wymaga podania przez pacjenta numeru PESEL oraz numer telefonu/email • Treść wiadomości wysyłanej do pacjenta zawiera kod oraz dowolny tekst definiowany w graficznym edytorze • System RIS udostępnia poprzez oferowane rozwiązanie opisy badań diagnostycznych podpisane kwalifikowanym certyfikatem osoby autoryzującej opis
Integracja z systemem RIS - Weryfikacja	• System RIS weryfikuje wprowadzone dane w bazie danych systemu RIS • Poprawna weryfikacja powoduje wysłanie jednorazowego kodu dostępu w formie wiadomości SMS/email umożliwiającego zalogowanie się do PORTALU
Integracja z EDM	• Funkcje dodatkowe: Wykonawca zobligowany jest do integracji systemu RIS funkcjonującym w szpitalu z modułem Elektronicznej Dokumentacji Medycznej w zakresie: ◦ System RIS/PACS powinien zasilać repozytorium EDM dokumentami typu "Opis badania radiologicznego” ◦ System RIS/PACS umożliwia, by w dokumencie elektronicznym przekazywany był link do wglądu badania w formie DICOM oraz w postaci referencyjnej ◦ System ma mieć możliwość wygenerowania opisu badania podpisanego kwalifikowanym podpisem elektronicznym lekarza opisującego. System ma obsługiwać formaty podpisu PAdES oraz XAdES ◦ Podczas podpisywania opisu badania system ma mieć możliwość prezentacji opisu zgodnie z szablonami dokumentów elektronicznych opublikowanych na stronach CEZ ◦ System RIS/PACS ma mieć możliwość każdorazowej modyfikacji opisu, który wymaga wytworzenia nowej wersji dokumentu elektronicznego i wysłania do EDM ◦ System RIS/PACS ma mieć możliwość usunięcia opisu. Spowoduje to oznaczenie jako nieaktywny dokumentu w ramach EDM • System musi umożliwiać przypisanie badania do wybranego lekarza do opisu • System musi umożliwiać przypisanie badania do wybranego personelu do przepisania • System musi umożliwiać, by użytkownik mógł przypisać do siebie nieprzypisane badania • System musi umożliwiać otwarcie okna opisu, który wysyła komunikat do przeglądarki z żądaniem wyświetlenia zdjęć opisywanego badania

	• System musi umożliwiać, by okno opisu posiadało możliwość dodania szablonów opisów globalnych dla gabinetu, dostępnych dla wszystkich oraz szablonów poszczególnych lekarzy • System musi umożliwiać, by użytkownik miał możliwość oznaczenia skrótem szablonu opisu • System musi umożliwiać, by użytkownik miał możliwość wyświetlenia podpowiedzi/szablonów pod skrótem klawiszowym • System musi umożliwiać, by użytkownik miał możliwość uzupełnienia kodu ICD10 opisu • System ma posiadać opcję kopiowania ICD10 ze skierowania do opisu (konfigurowalne przez administratora) • System ma posiadać opcję blokady zatwierdzenia opisu jeśli lekarz nie wybrał kodu ICD 10 (konfigurowalne przez administratora) • System musi umożliwiać, by użytkownik w oknie opisu widział uwagi z rejestracji oraz uwagi od technika • System musi umożliwiać, by użytkownik mógł wyświetlić w bocznym oknie poprzednie badania i opisy pacjenta • System musi umożliwiać, by użytkownik podczas opisu mógł wyświetlić szczegółowe dane pacjenta, oraz badania • System musi umożliwiać, by użytkownik mający odpowiednie uprawnienia mógł zatwierdzić opis, bądź zapisać w celu dalszej pracy. • System musi umożliwiać, by użytkownik z odpowiednimi uprawnieniami miał możliwość zmiany przypisania badań do lekarzy • System ma mieć możliwość każdorazowej modyfikacji opisu, który wymaga wytworzenia nowej wersji dokumentu elektronicznego i wysłania do EDM

6. Pakiet / Zadanie nr 6. Dostarczenie i uruchomienie modułów HIS, systemu autoryzacji wyników badań laboratoryjnych oraz e-Usług.

6.1. Wymagania ogólne i opis rozwiązania

- Wykonawca zobowiązany jest dostarczyć licencje na moduły oprogramowania HIS w ilości 5 sztuk. Szczegóły funkcjonalności modułów i ich ilości opisano w punkcie 6.2.1.
- Wykonawca dokona konfiguracji każdej wskazanej przez Zamawiającego stacji roboczej pod kątem możliwości uruchomienia na niej aplikacji do podpisywania wyników badań laboratoryjnych podpisem kwalifikowanym.
- Skonfigurowanie modułu LIS Zamawiającego do generowania dokumentów w standardzie PIK HL7 CDA.
- Konfiguracja EDM Zamawiającego do odkładania wyników w standardzie PIK HL7 CDA.
- Modyfikacja słownika kontrahentów o dane niezbędne do prawidłowego wygenerowania dokumentów zgodnie z wymaganiami EDM.
- Rekonfiguracja listy procedur i metod badań wykonywanych w systemie LIS Zamawiającego.
- Uzupełnienie słownika personelu wykonującego badania o dane niezbędne do prawidłowego wygenerowania dokumentów zgodnie z wymaganiami EDM.
- Instalacja i wdrożenie interfejsów do poszczególnych e-Usług (przygotowanie środowiska i platformy interfejsów w zakresie udostępnianych rejestrów usług medycznych, personelu, lokalnego EDM).
- Dla e-Usług przygotowanie:
  - Danych portalowych,
  - Środowiska do integracji,
  - Kanałów VPN,
  - Środowiska serwerowego,

- Przygotowanie testów.

- Wykonawca zorganizuje prace tak, aby zminimalizować ich wpływ na ciągłość funkcjonowania działalności systemów informatycznych Zamawiającego.

6.2. Specyfikacja szczegółowa

6.2.1. Licencje (moduły) do systemu HIS – 1 kpl.

L.p.	Nazwa modułu	Ilość licencji
1	Blok operacyjny	2
2	Apteka	2
3	Punkt pobrań	1

Funkcjonalność modułu	Ilość licencji
Blok Operacyjny	2

Funkcjonalność:

- System powinien umożliwiać wyłączanie niewykorzystanych zakładek
- System powinien umożliwiać zmianę kolejności prezentacji zakładek
- System powinien umożliwiać planowanie zabiegów operacyjnych dla pacjentów przebywających na oddziale
- System powinien umożliwiać planowanie zabiegów operacyjnych podczas wizyty w gabinecie lekarskim, pacjentom nie przebywającym w szpitalu
- System musi umożliwić jednoznaczne oznaczanie zabiegów:
  - zaplanowanych i niewykonanych
  - niezakończonych
  - anulowanych
- System powinien umożliwiać planowanie zabiegów dla pacjentów kierowanych na zabieg z innych jednostek organizacyjnych
- System musi umożliwiać zaplanowanie i odnotowanie danych wykonania operacji wielonarządowych
- System musi umożliwiać dokonanie klasyfikacji lekarskiej (chirurgicznej) do zabiegu obejmującej, co najmniej:
  - rodzaj planowanego zabiegu
  - tryb zabiegu (planowy, przyspieszony, pilny, natychmiastowy)
  - rozpoznanie przedoperacyjne ICD9 oraz opisowe
  - dostęp do pola operacyjnego z wykorzystaniem definiowalnego słownika
  - wymagane ułożenie pacjenta z wykorzystaniem definiowalnego słownika, z możliwością wyboru wielu pozycji
  - datę kwalifikacji
  - wskazanie ze słownika personelu, lekarza dokonującego kwalifikacji
  - możliwość załączenia formularza definiowanego przez użytkownika
- Musi istnieć możliwość rejestracji danych kwalifikacji z poziomu oddziału i z poziomu bloku operacyjnego
- Musi istnieć możliwość uproszczonego zlecania zabiegów przeprowadzanych w trybie nagłym
- System musi umożliwić zaplanowanie przerw technicznych pomiędzy zabiegami (czas na przygotowanie i posprzątanie Sali)
- System musi umożliwić prezentowanie na planie dziennym i okresowym operacji, informacji o tym czy pacjent przebywa już w szpitalu oraz czy wykonana została kwalifikacja anestezjologiczna
- System musi umożliwić skonfigurowanie kontroli limitów wykonań dla zdefiniowanych grup zabiegów operacyjnych
- System musi umożliwiać dokonanie klasyfikacji anestezjologicznej, co najmniej w zakresie odnotowania:
  - rodzaju planowanego znieczulenia z wykorzystaniem słownika rodzajów znieczulenia z możliwością definiowania własnych rodzajów znieczulenia
  - klasyfikacji pacjenta wg skali ASA

- opisu kwalifikacji
- daty kwalifikacji
- wskazania lekarza dokonującego kwalifikacji
- możliwości rejestracji danych kwalifikacji z poziomu oddziału i z poziomu bloku operacyjnego

- Planowanie powinno się odbywać w oparciu o terminarze bloku i sal operacyjnych
- Po rejestracji zakończenia zabiegu, jeśli jego czas trwania był inny niż zaplanowano, system powinien zaktualizować terminarz dla pozostałych, zaplanowanych zabiegów
- System musi umożliwić planowanie zabiegu operacyjnego w tym wpisanie:
  - daty zabiegu, bloku operacyjnego i sali operacyjnej
  - materiałów
  - zamówienia preparatów krwi wymaganych do przeprowadzenia zabiegu z możliwością wydrukowania zamówienia do banku krwi
  - składu zespołu zabiegowego i anestezjologicznego z wykorzystaniem słownika personelu z możliwością określenia definiowania roli członków personelu
  - możliwość rejestracji danych planu z poziomu oddziału i z poziomu bloku operacyjnego
- System musi umożliwić odnotowanie rozpoczęcia realizacji zabiegu operacyjnego w chwili zarejestrowania przyjęcia pacjenta na blok operacyjny
- Musi istnieć możliwość obsługi listy zabiegów bloku operacyjnego, obejmującej:
  - dostęp do aktualnych i archiwalnych danych pacjentów
  - modyfikacja danych pacjentów
- System musi umożliwiać wyszukiwanie zabiegów na liście zabiegów bloku operacyjnego wg różnych kryteriów, w tym:
  - statusu zabiegu (planowany, w trakcie realizacji, opieka pooperacyjna, przekazany na oddział, anulowany)
  - danych pacjenta (nazwisko, imię, PESEL)
  - identyfikatorze pacjenta
  - trybu zabiegu
  - rodzaju zabiegu
  - planowanych i rzeczywistych dat wykonania zabiegu
  - bloku i sali operacyjnej
    jednostki zlecającej
  - Wykazu Zabiegów
    składu zespołu operacyjnego (operatora, instrumentariusza, anestezjologa, pielęgniarki anestezjologicznej)
  - przeglądu zabiegów zaplanowanych na dzisiaj i/lub jutro
- System musi umożliwiać przyjęcie pacjenta na blok operacyjny i odnotowanie związanych z tym danych tj.:
  - czas przyjęcia i osoby przyjmującej
  - wpis do Księgi Bloku operacyjnego
- System musi umożliwić odnotowanie danych medycznych przeprowadzonego zabiegu w tym:
  - rodzaju wykonanego zabiegu
  - czasu trwania zabiegu
    rozpoznania pooperacyjnego ICD10 i opisowego
  - procedur medycznych z możliwością automatycznego dodania procedur powiązanych z przeprowadzonym zabiegiem
  - opisu wykonanego zabiegu wraz z lekarzem opisującym
  - składu zespołu zabiegowego domyślnie uzupełnianego na podstawie planu
  - czasu pracy zespołu operacyjnego. Jeśli czas pracy nie zostanie wpisany powinien być uzupełniony przez system na podstawie czasu rozpoczęcia i zakończenia zabiegu
  - możliwość załączenia formularza definiowanego przez użytkownika
  - możliwość dołączania załączników w postaci dowolnych plików (np. skany dokumentów, pliki dźwiękowe i wideo)
  - odnotowanie przetoczeń krwi i preparatów krwiopochodnych z wpisem do księgi transfuzyjnej, odnotowanie powikłań po przetoczeniu
  - zużytych materiałów:
    - z wykorzystaniem kodów kreskowych lub poprzez manualny wybór pozycji ze słownika
    - z możliwością automatycznego dodania materiałów z planu
    - z możliwością automatycznego dodania materiałów powiązanych z wykonanym zabiegiem
    - z możliwością automatycznego dodania zestawu narzędzi powiązanych z wykonywanym zabiegiem
    - możliwość rejestracji danych z poziomu oddziału i z poziomu bloku operacyjnego
- System na liście zabiegów oraz na liście opieki pooperacyjnej powinien wyróżniać pacjentów po transfuzji krwi, dla których nie została uzupełniona dokumentacja jej dotycząca
- Oprócz głównego opisu operacji system musi umożliwiać wprowadzanie dodatkowych uwag dotyczących przebiegu zabiegu, opatrzonych datą i danymi osoby wprowadzającej

- Po wykonaniu zabiegu, system powinien umożliwiać zmianę procedury głównej zabiegu
- Jeśli nie zostały wpisane dane lekarza operującego to system powinien podpowiadać operatora na podstawie danych lekarza opisującego zabieg
- System musi umożliwić wprowadzenie informacji dotyczących przygotowania pacjenta do zabiegu
- System musi umożliwiać wprowadzenie informacji dotyczących powikłań pooperacyjnych
- System musi umożliwiać wprowadzenie w ramach opieki pooperacyjnej pacjenta, danych opieki pielęgniarskiej
- System musi umożliwić definicję rodzajów znieczulenia
- System musi umożliwić rejestrację danych znieczulenia, w tym:
  - czasu znieczulenia
  - czasu anestezjologicznego
  - rodzaju przeprowadzonego znieczulenia domyślnie wypełnianego na podstawie kwalifikacji z możliwością edycji
  - opisu znieczulenia ze wskazaniem osoby opisującej
  - zespołu anestezjologicznego domyślnie uzupełnionego na podstawie planu
  - czasu pracy zespołu anestezjologicznego. Jeśli czas pracy nie został wpisany system podpowiada na podstawie czasu anestezjologicznego lub jeśli czas anestezjologiczny nie jest obsługiwany na podstawie czasu znieczulenia.
  - podanych leków:
    - z wykorzystaniem kodów kreskowych lub poprzez manualny wybór pozycji ze słownika
    - z możliwością automatycznego dodania leków powiązanych z wykonanym zabiegiem
- System powinien umożliwić dodawanie pakietów leków i materiałów podczas rejestracji danych dotyczących wykonania operacji
- System powinien umożliwić grupowe dodawanie procedur medycznych (wielowybór) w danych znieczulenia
- System powinien umożliwić grupowe dodawanie procedur medycznych (wielowybór) w danych wykonania operacji oraz w danych opieki pooperacyjnej
- System musi wspomagać opiekę pooperacyjną w zakresie:
  - ewidencji czasu trwania opieki pooperacyjnej oraz lekarza przyjmującego
  - ewidencji wykonanych procedur
  - ewidencji podanych leków i zużytych materiałów
  - obsługi tacy leków
  - oceny stanu pacjenta z wykorzystaniem zmodyfikowanej skali Aldrete'a
  - opisu powikłań znieczulenia
  - opisu zaleceń pooperacyjnych
  - ewidencji daty przekazania pacjenta na oddział wraz ze wskazaniem lekarza przekazującego
- System musi umożliwiać realizację reoperacji pacjenta bezpośrednio po właściwej operacji bez konieczności przekazywania pacjenta na oddział
- System powinien umożliwić wydruk szablonu karty znieczulenia z danymi nagłówkowymi pacjenta
- System powinien umożliwić wydruk szablonu karty pooperacyjnej z danymi nagłówkowymi pacjenta
- System powinien umożliwić prezentacja graficzna wprowadzonych wyników pomiarów, procedur i leków na jednej osi czas (co umożliwi obserwację zależności pomiędzy podaniami leków i wykonaniem procedur a wynikami pomiarów)
- System musi umożliwiać prowadzenie Wykazów Operacji w zakresie:
  - możliwość definiowania księgi dla bloku operacyjnego, dla sali operacyjnej oraz dla grupy zabiegów
  - przegląd Wykazów Operacji wg. różnych kryteriów, w tym:
    - danych pacjenta (nazwisko, imię, PESEL)
    - trybu zabiegu
    - rodzaju zabiegu
    - dat wykonania zabiegu
    - bloku i sali operacyjnej
    - oddziału zlecającego
    - Wykazu Zabiegów
    - roku księgi
    - zakresu numerów księgi
    - składu zespołu operacyjnego (operatora, instrumentariusza, anestezjologa, pielęgniarki anestezjologicznej)
  - wydruk księgi bloku operacyjnego
- System musi umożliwić przekazanie pacjenta na oddział opieki pooperacyjnej bez wprowadzonych danych realizacji zabiegu; z możliwością późniejszego uzupełnienia danych.
- System musi wspomagać prowadzenie dokumentacji zabiegu operacyjnego, w tym:
  - protokół zabiegu operacyjnego
  - protokół przekazania pacjenta na oddział

- możliwość uzupełniania dokumentacji o materiały elektroniczne - skany dokumentów, zdjęcia, pliki dźwiękowe oraz wideo
- opcjonalne przechowywanie wszystkich wersji utworzonych dokumentów

- Musi istnieć możliwość definiowania własnych szablonów wydruków
- Musi istnieć możliwość obsługi raportów wbudowanych, w tym:
  - raport z wykonań zabiegów operacyjnych z uwzględnieniem kryteriów: czas wykonania zabiegu, Wykazu Zabiegów, salę operacyjną, jednostkę zlecającą oraz rodzaj operacji
- System musi umożliwiać wybór formatu wydruku raportów, przynajmniej w zakresie: pdf, xls, xlsx.
- Musi istnieć możliwość definiowania własnych wykazów
- Musi istnieć możliwość projektowania formularzy dokumentacji medycznej
- System musi zapewnić integrację z innymi modułami systemu medycznego w zakresie:
  - dostępu do historii choroby i dokumentacji medycznej bieżącego pobytu szpitalnego
  - rejestracji kart zakażeń
  - automatycznej aktualizacji stanów magazynowych przy ewidencji leków i materiałów
  - przekazywanie zamówień na krew i preparaty krwiopochodne do banku krwi
  - przekazywanie preparatów krwi z banku krwi na blok operacyjny
  - aktualizacja stanów magazynowych banku krwi na podstawie danych z bloku operacyjnego
  - wzajemnego udostępniania informacji o zleconych badaniach i konsultacjach
  - przeglądu wyników zleconych badań i konsultacji
  - przeglądu wszystkich poprzednich hospitalizacji pacjenta i wizyt w przychodni
  - udostępniania informacji o wykonanych świadczeniach, podanych lekach i zużytych materiałach dla celów statystycznych i rozliczeniowych
- System musi umożliwić pracę współbieżną użytkowników w zakresie pracy na tym samym zestawie danych. Ponadto system musi umożliwiać rozwiązywanie konfliktów występujących podczas jednoczesnej pracy na tym samym zestawie danych.
- Udostępnianie danych dotyczących czasu pracy personelu na bloku operacyjnym oraz informacji o ośrodkach kosztów sal zabiegowych do wykorzystania w systemie KP.

Apteka	2

Funkcjonalność:

- Obsługa magazynu leków apteki
- Konfiguracja magazynu apteki:
  - System musi umożliwiać zastosowanie słowników leków, grup ATC i nazw międzynarodowych do ewidencji obrotu lekami i materiałami
  - System musi umożliwiać definiowanie dwupoziomowej hierarchii grup leków/materiałów
  - System musi umożliwiać definiowanie grup materiałów dla całego systemu i dla poszczególnych magazynów
  - System musi umożliwiać prowadzenie rejestru leków i materiałów dla każdego magazynu odrębnie
  - System musi umożliwiać wyszukiwanie leków/materiałów za pomocą skanowania kodów EAN13 i EAN128
  - System musi umożliwiać definiowanie własnych rodzajów dokumentów dla poszczególnych rodzajów przyjęć, wydań innych czynności (np.. Rozchód darów, przyjęcie bezpłatnych próbek itp.)
  - System musi umożliwiać prowadzenie numerowania dokumentów wg zdefiniowanego szablonu zawierającego rok, miesiąc, symbol dokumentu, kod użytkownika
  - System musi umożliwiać drukowanie etykiety na szuflady w magazynie apteki
- System powinien umożliwiać wyróżnienie leków których dodania do receptariusza jednostki wymaga odrębnych uprawnień
- System musi umożliwiać sporządzanie zamówień doraźnych do dostawców środków farmaceutycznych i materiałów medycznych
- System musi umożliwiać umieszczenie informacji w pozycji zamówienia o tym, że zamówienie może być zrealizowane za pomocą odpowiednika zamawianego leku
- System musi umożliwiać rejestrowania przyjęcia dostaw leków i materiałów medycznych od dostawców, w szczególności:
  - automatyczne uzupełnienie dokumentu dostawy na podstawie faktury w formie elektronicznej
  - możliwość manualnej rejestracji dokumentów przyjęcia, w tym dostaw dla których nie dostarczono faktury
- System musi umożliwiać rejestrowanie dokumentów sporządzenia preparatów laboratoryjnych, preparatów galenowych, leków recepturowych ora płynów infuzyjnych
- System powinien umożliwić automatyczne generowanie numeru serii dla dokumentu produkcji
- System powinien kontrolować daty ważność składnika dodawanego do leku recepturowego, jeśli data ważności składnika będzie przeterminowana w momencie produkcji oraz data ważności składnika będzie przeterminowana

w momencie podania leku recepturowego to system powinien informować użytkownika o tym fakcie stosownym komunikatem
- System musi umożliwiać przegląd składu leku recepturowego w dokumencie produkcji
- System musi umożliwiać rejestrowanie dokumentu sporządzenia roztworów spirytusowych
- System musi umożliwiać rejestrowanie dokumentów importu docelowego zakładowego i indywidualnego
- System musi umożliwiać rejestrowanie dokumentów zwrotu leków i materiałów medycznych z apteczek oddziałowych z aktualizacją ich stanów
- System umożliwia blokowanie wprowadzania zmian w dokumentach z innego dnia, niż bieżący.
- System musi umożliwiać rejestrowanie dokumentów przyjęcia darów
- System musi umożliwiać rejestrowanie danych osoby dostarczającej próbkę oraz nazwę podmiotu odpowiedzialnego w dokumencie przyjęcia próbki
- System musi umożliwiać rejestrowanie numeru protokołu w dokumencie przyjęcia leku wykorzystywanego w programie badań klinicznych
- System musi umożliwiać rejestrowanie pozycji dokumentu przychodu przez skanowanie kodu EAN13/EAN128. W przypadku odczytania kodu leku który nie znajduje się jeszcze w dokumencie system automatycznie tworzy nową pozycję dokumentu.
- System powinien umożliwić wydruk informacji o przetargach I zamówieniach na dokumencie przychodu
- System powinien umożliwić weryfikację różnic pomiędzy pozycją przychodu, a pozycją przetargową lub pozycją zamówienia.
- System powinien umożliwić wprowadzenie aneksu z ilością mniejszą niż już zrealizowana
- System powinien umożliwiać możliwość rejestrowania przychodów niefakturowanych za pomocą wybranych dokumentów PZ
- System musi umożliwiać rejestrowanie dokumentów korygujących do dokumentów przyjęcia leków i materiałów
- System musi umożliwiać rejestrowanie korekty pozycji dokumentu przyjęcia również w przypadku częściowej korekty tej pozycji
- System powinien umożliwić potwierdzenie przyjęcia zlecenia żywienia pozajelitowego przez Pracownie
- System powinien umożliwić przekazanie leku/worka żywienia pozajelitowego do jednostki zlecającej
- System musi umożliwiać realizację zleceń na leki cytostatyczne poprzez zarejestrowanie dokumentu produkcji leku cytostatycznego i dokument wydania leku z Apteki do Apteczki.
- System powinien wyświetlać wagę pacjenta
- System musi umożliwić obsługę wydania leku pacjentowi do domu, w ramach schematu leczenia.
- System musi umożliwiać rejestrowanie wydań leków i materiałów medycznych:
- System musi umożliwiać rejestrowanie wydań za pomocą dokumentów RW i MM na podstawie zamówień elektronicznych lub papierowych z Apteczek Oddziałowych
- System musi umożliwiać ewidencję wydań poprzez skanowanie kodów EAN13 i EAN128
- System musi umożliwiać definiowanie rodzajów akceptacji dla rzutów.
- System musi umożliwiać określenie dla rzutu rodzaju wymaganej akceptacji.
- System musi informować użytkownika podczas rejestrowania zamówienia o rodzaju wymaganej akceptacji właściwej dla rzutu do którego przypisany jest zamawiany lek.
- System musi umożliwiać potwierdzenie przez oddział realizacji zamówienia
- System powinien umożliwić zawężenia listy zamówień do tych, w których istnieją leki/materiały obsługiwane przez bieżący magazyn
- System musi umożliwiać zarejestrowanie dokumentu rozchodu wewnętrznego (bez przychodu u zamawiającego) leku na podstawie zamówienia.
- System powinien posiadać możliwość rozchodu całości aktualnych stanów magazynu dla wybranych leków/materiału jednym kliknięciem
- System musi umożliwiać rejestrowanie dokumentów wydania na zewnątrz
- System musi umożliwiać rejestrowanie dokumentów zwrotu do dostawcy
- System musi umożliwiać rejestrowanie dokumentu zwrotu korekty zwrotu do dostawcy
- System musi umożliwiać rejestrowanie dokumentu ubytki i straty nadzwyczajne
- W dokumencie przesunięcia międzymagazynowego system powinien umożliwić dodanie pozycji z innych dokumentów
- System musi umożliwiać rejestrowanie dokumentu korekty wydania środków farmaceutycznych
- System musi umożliwiać definiowanie i wykonywanie kontroli limitów wartościowych wydań leków i środków medycznych do komórek organizacyjnych
- System musi umożliwiać prezentację ilości w postaci ułamkowej
- System musi umożliwiać rezerwowanie określonej ilości leków lub materiałów dla wskazanego pacjenta
- System musi umożliwiać korektę stanów magazynowych:
- System musi umożliwiać korektę stanów magazynowych (ilościowo i jakościowo) na podstawie arkusza spisu z natury rejestrowanego z dokładnością do dostawy lub asortymentu

- System musi umożliwiać generowanie arkusza spisu z natury
- System musi umożliwiać bieżącą korektę stanów magazynowych
- System musi podczas generowanie dokumentu remanentu na podstawie spisu z natury sprawdzić czy stwierdzono różnice inwentaryzacyjne. W przypadku braku różnic musi poinformować o tym użytkownika
- System musi umożliwiać odnotowanie wstrzymania lub wycofanie leku z obrotu
- System musi kontrolować daty ważności wydawanych leków. System musi umożliwiać zdejmowanie ze stanów leków przeterminowanych za pomocą wskazanych dokumentów.
- System musi oznaczać na liście kolorem/symbolem umowy, dla których zbliża się koniec terminu ważność.
- System w generatorze zamówień do kontrahentów musi umożliwiać tworzenie jednego zamówienia dla wielu umów.
- System musi umożliwiać oznaczenie danych kontrahenta w związku z ograniczeniem przetwarzania jego danych lub roszczeniem.
- System musi umożliwiać anonimizację danych kontrahenta.
- System musi umożliwić dopisanie do spisu z natury pozycji, dla których nie odnotowano obrotów w danym magazynie.
- System musi umożliwiać przegląd bieżących stanów magazynowych jak i na wskazany dzień
- System musi umożliwić weryfikację przekroczenia wartości procentowej limitu ustawionego dla magazynu.
- System musi umożliwiać wsparcie obsługi i kontroli zamówień (w tym publicznych) w zakresie:
- - przekazywanie listy asortymentowo - wartościowej leków do modułu realizującego funkcjonalność Obsługi zamówień i przetargów,
- - pobieranie zwycięskiej oferty (umowy),
- - kontrola realizacji dostaw i poziomu cen w ramach zwycięskiej oferty (umowy).
- System w generatorze zamówień do kontrahentów musi umożliwiać tworzenie jednego zamówienia dla wielu umów.
- System powinien umożliwić wpisanie dodatkowej treści e-mail dla zamówienia zewnętrznego (zamówienie do Kontrahenta) oraz umieszczenie na wydruku nr zamówienia
- System powinien umożliwić generowanie pozycji do zamówień zewnętrznych na podstawie wydań w zadanym okresie
- System musi współpracować z blistrownicą przepakowującą leki w dawki jednostkowe (unit dose)
- System musi prezentować informację o stanie realizacji zlecenia w unit dose
- System powinien umożliwiać zamawianie leków w systemie UnitDose dla zleceń doraźnych (bez określenia pory podania).
- System musi wspomagać obsługę zleceń na leki cytostatyczne w zakresie co najmniej:
  - realizacja zamówienia na produkcję leku cytostatycznego
  - automatycznego wycofania produkcji cytostatyku z równoczesnym przekazaniem informacji o anulowaniu do systemu Pracownia Cytostatyków Eskulap
  - możliwości wygenerowania raportu zawierającego szczegóły zamówień wystawionych przez Pracownie Cytostatyków, z możliwością ograniczenia tylko do zamówień oczekujących na realizację
- System musi wspomagać obsługę produkcji preparatów żywienia pozajelitowego w zakresie co najmniej:
  - wyliczanie podstawowych parametrów preparatu żywienie pozajelitowego oraz kontrolowanie wartości granicznych, co najmniej w zakresie stężenia krytycznego i osomolarności
  - generowania etykiet
- System powinien umożliwić integracje z systemem zewnętrznym MEDIM
- System musi generować zestawienia
  - na podstawie rozchodów
  - na podstawie przychodów
  - na podstawie stanów magazynowych
  - możliwość wydruku do XLS
  - raport realizacji zamówień wewnętrznych
- System musi posiadać możliwość utworzenia i wydruku raportu na podstawie rozchodów dla grup analitycznych.
- System musi umożliwiać planowanie realizacji zamówień wewnętrznych.
- System umożliwia automatyczne utworzenie i wysłanie zapotrzebowania do apteki na podstawie zlecenia lekarskiego.
- System musi posiadać możliwość przekazywania wszystkich wydruków do plików w formacie PDF
- System musi umożliwiać definiowanie własnych raportów
- System musi wspomagać użytkownika w zakresie decyzji farmaceutycznych w zakresie przechowywania informacji o leku
- System:
  - umożliwia rejestrowanie dokumentów sporządzenia preparatów laboratoryjnych, preparatów galenowych, leków recepturowych oraz płynów infuzyjnych

- umożliwia realizację zleceń na leki cytostatyczne poprzez zarejestrowanie dokumentu produkcji leku cytostatycznego i dokument wydania leku z Apteki do Apteczki
- umożliwia zarządzania lekami własnymi pacjenta
- umożliwia zarządzania stratami i utylizacją leków
- wspomaga użytkownika w zakresie decyzji farmaceutycznych w zakresie wstrzymanie, wycofanie decyzją GIF
- musi podczas generowanie dokumentu remanentu na podstawie spisu z natury sprawdzić czy stwierdzono różnice inwentaryzacyjne. W przypadku braku różnic musi poinformować o tym użytkownika
- umożliwia odnotowywanie działań niepożądanych
- umożliwia definiowanie receptariusza szpitalnego

- System musi umożliwiać integrację z innymi modułami realizującymi funkcjonalności w zakresie:
  - Finanse – Księgowość:
    - dostępność funkcji wartościowego, syntetycznego zapisu obrotu materiałowego na kontach księgi głównej FK
    - możliwość zapisu dokumentów rozchodowych (koszty) na poziomie wydania z magazynu apteki
    - możliwość zapisu dokumentów rozchodowych (koszty) na poziomie wydania z magazynu apteczki oddziałowej
    - możliwość eksportu dokumentów rozchodu wewnętrznego w formacie OSOZ-EDI
    - możliwość elastycznego tworzenia wzorców eksportu do FK
    - możliwość wykorzystania słowników FK: kontrahentów, rodzajów kosztów, ośrodków powstawania kosztów
  - Rachunek kosztów leczenia:
    - w zakresie udostępnienia indeksu leków i danych o aktualnych cenach leków do określenia normatywów materiałowych świadczeń (w zakresie leków)
  - Ruch Chorych, Przychodnia:
    - w zakresie skorowidza pacjentów
- System musi umożliwić rozliczenie dostaw z całego miesiąca jedną fakturą
- System musi umożliwić domyślne otwarcie nowego okresu rozliczeniowego z pierwszym dniem nowego miesiąca
- System musi umożliwiać kontrolę interakcji pomiędzy składnikami leków recepturowych
- System musi umożliwiać analizę interakcji pomiędzy składnikami leków wydanych pacjentowi
- System musi umożliwiać definiowanie zamienników dla wybranych leków
- System musi umożliwiać przypisywanie leków do grup odpowiedników/odpowiedników
- System powinien uniemożliwiać wprowadzenie karty leku/materiału o tym samym indeksie
- System musi umożliwiać kontrolę interakcji pomiędzy składnikami leków recepturowych
  - konfigurację magazynu depozytów obejmującą możliwość definiowania dokumentu oraz możliwość oraz karty materiału depozytowego
  - obsługę dokumentów:
    - przyjęcie materiałów w depozyt
    - faktura depozytowa
    - korekta faktury depozytowej
    - rozchód depozytowy na pacjenta
    - rozchód depozytowy bez pacjenta
    - korekta rozchodu depozytowego
  - zamówienia do dostawcy:
    - generowanie zamówienia na podstawie rozchodu depozytowego
    - tworzenie zamówienia depozytowego bez wskazania pacjenta
  - Kontrola realizacji zamówień do dostawców oraz umów przetargowych
  - wprowadzanie i edycja numeru pozycji na fakturze depozytowej
  - Raporty:
    - na podstawie przychodów
    - na podstawie rozchodów
    - raport z produkcji cytostatyków
    - możliwość zapisu w formacie xls
  - eksport do Systemu Finansowo Księgowego
- System musi umożliwiać przegląd historii eksportów dekretów do FK
- System musi umożliwiać przeglądu historii eksportów VAT do FK
- System musi za komunikację z zakresie JPK, w szczególności:
  - przygotowanie i wysłanie komunikatu JPK_MAG
  - odbiór potwierdzenia odbioru (UPO)
- System musi umożliwiać integrację z szafami lekowymi.
- System musi umożliwiać powiązanie magazynu z szafami lekowymi.
- System powinien uniemożliwiać zarejestrowanie zużycia leku, który został wydany z Apteki dla innego pacjenta.

- System powinien umożliwić wyliczenie liczby wydań leków/materiałów z podziałem na OPK.
- System musi umożliwiać weryfikację autentyczności leków w systemie PLNMV.
- System musi umożliwiać weryfikację autentyczności leków w systemie PLNMV odrębnie dla każdej apteki zarejestrowanej w Rejestrze Aptek
- System musi przechowywać informacje o wyniku weryfikacji każdego niepowtarzalnego identyfikatora
- System musi umożliwiać wykonanie następujących operacji w ramach weryfikacji leków:
  - weryfikacja niepowtarzalnego identyfikatora
  - wycofanie niepowtarzalnego identyfikatora jako użycie/wydanie
  - wycofanie niepowtarzalnego identyfikatora jako próbka
  - wycofanie niepowtarzalnego identyfikatora jako zniszczenie
- System powinien umożliwić anulowanie zużycia leku w systemie Krajowej Organizacji Weryfikacji Autentyczności Leków (KOWAL) za pomocą manualnego wprowadzenia niezbędnych informacji
- System musi wykonywać operację weryfikacji automatycznie po operacji odczytania kodu Data Matrix z opakowania leku za po pomocą skanera kodów
- System musi umożliwiać rejestrowanie i przechowywanie w systemie informacji o Unikalnych Identyfikatorów Wyrobów Medycznych będących w obrocie podmiotu medycznego.
- Rejestrowanie identyfikatorów odbywa się za pomocą skanowania kodów 2D.
- System musi umożliwiać wygenerowanie i przesłanie komunikatu obrotów i stanów do Zintegrowanego Systemu Obrotu Produktami Leczniczymi (ZSMOPL)
- System powinien pobrać na żądanie ze ZSMOPL informacje o stanach leków w aptece
- System powinien zaprezentować różnice pomiędzy stanami w ZSMOPL i stanami w aptece
- System powinien wygenerować komunikat do ZSMOPL zawierający informacje a aktualnych stanach apteki dla wybranych leków
- System musi odebrać i zapisać identyfikator komunikatu nadany przez ZSMOPL
- System musi umożliwiać wygenerowanie i wysłanie komunikatu obrotów i stanów do ZSMOPL na żądanie użytkownika
- System musi umożliwiać wygenerowanie i wysłanie komunikatu obrotów i stanów do ZSMOPL automatycznie i cyklicznie
- System musi umożliwiać generowanie i wysyłanie korekt komunikatów do systemu ZSMOPL.
- System powinien umożliwić wygenerowanie korekty raportu do systemu ZSMOPL z modyfikacją serii lub daty ważności
- System powinien umożliwić raportowanie obrotów i strat do systemu ZSMOPL
- System powinien umożliwiać przeprowadzenie testu poprawności działania skanera kodów DataMatrix w zakresie weryfikacji autentyczności leków
- System musi umożliwiać przegląd listy transakcji dla wygenerowanego komunikatu
- System musi umożliwiać wygenerowanie komunikatu stanów i obrotów odrębnie dla każdej apteki zarejestrowanej w Rejestrze Aptek
- System musi umożliwiać import danych z rejestru Hurtowni Farmaceutycznych
- System musi umożliwiać aktualizację listy hurtowni prowadzonych przez kontrahenta na podstawie Rejestru Hurtowni Farmaceutycznych
- System musi umożliwiać przeglądanie decyzji i komunikatów Głównego Inspektoratu Farmaceutycznego
- System musi umożliwiać aktualizację online słownika hurtowni na podstawie Rejestru Hurtowni Farmaceutycznych CeZ.
- System musi umożliwiać automatyczne wysłanie powiadomienia do Apteki o wysłaniu zamówienia z Apteczki Oddziałowej
- System musi umożliwiać wyświetlenie powiadomień o umowach z apteki, dla których kończy się termin ważności.
- Akceptacja zamówień do dostawców:
  - System powinien umożliwić obsługę dwustopniowego proces akceptacji zamówień do dostawców
  - System powinien umożliwić filtrowanie zamówień do dostawców według statusu akceptacji
  - System powinien umożliwić odrzucenie zamówienia wysłanego do akceptacji
  - System powinien umożliwić wpisanie powodu odrzucenia zamówienia wysłanego do akceptacji
  - W zamówieniach do dostawców system powinien umożliwić przegląd historii akceptacji zamówienia
- System powinien umożliwić zmianę status dla zamówienia wsyłanego do dostawcy.

Punkt pobrań	1

Funkcjonalność:

- System powinien umożliwiać zarządzanie zleceniami na badania laboratoryjne, w szczególności:
  - przyjmowanie zleceń badań laboratoryjnych z podsystemu Ruch chorych i Przychodnia z możliwością określenia domyślnego punktu pobrań dla zleceniodawcy,

- wprowadzanie zleceń zewnętrznych, tak zwanych zleceń własnych, rejestrowanych bezpośrednio w Punkcie Pobrań
- możliwość wyszukiwania zleceń:
  - wg imienia i nazwiska oraz nr Pesel
  - wg daty zlecenia lub planowanej daty wykonania lub daty pobrania materiału
  - według jednostki zlecającej
  - oznaczonych jako pilne (CITO)
  - oznaczonych jako własne (zarejestrowane bezpośrednio w module Punkt Pobrań)
  - do ponownego pobrania materiału(są to zlecenia na badania, które wracają z Laboratorium, którym nie udało się zrealizować badania ze względu na błędy np. skrzep)
  - pacjentów, którzy są nosicielami niebezpiecznej bakterii
  - pacjentów, którzy mają oznaczoną izolację (pacjent izolowany ze względu wykryte zakażenie)
- na dostęp do zleceń archiwalnych pacjenta
- wyróżnianie zleceń CITO
- poprzez dobór odpowiednich materiałów niezbędnych do realizacji zlecenia
- poprzez wycofanie zlecenia

- System musi wspomagać obsługę pobrania materiału w zakresie:
  - podziału materiałów do pobrania wg jednostek wykonujących dane badanie (badania realizowane we własnych lub obcych laboratoriach)
  - podziału materiałów do pobrania wg lekarza zlecającego
  - rejestracji wysłania materiałów do laboratoriów
  - możliwości zastosowanie czytnika kart kodów kreskowych w celu oznakowania nr próbki pobranych materiałów
- System musi umożliwiać rejestrację pobranych materiałów, w tym:
  - automatyczne odnotowanie daty i godziny pobrania
  - odnotowanie osoby pobierającej materiał
  - odnotowanie dodatkowych uwag do pobrania
- Możliwość obsługi pobrania materiału w jednostce zlecającej
- Możliwość zmiany wykonawcy badania (jednostki wykonującej badanie)
- System umożliwia włączenie autoryzacji danych (wymagane podanie użytkownika i hasła) podczas zapisu pobrania materiału do badania
- System umożliwia określenie liczby dni, po których następuje automatyczne anulowanie niezrealizowanych zleceń
- Moduł Punkt Pobrań udostępnia grupowe anulowanie zleceń
- Obsługa zleceń do ponownego pobrania materiału
- Możliwość obsługi nieudanego pobrania materiału
- Możliwość dozlecania badań dla zleceń własnych (zleceń wystawionych bezpośrednio w Punkcie Pobrań)
- Możliwość wydruku etykiet dla pobranych próbek
- System umożliwia wydruk listy pobrań pogrupowanej wg nazwiska
- Obsługa i wydruk Księgi Pobrań
- Integracja z modułem Laboratorium w zakresie przetwarzania zleceń oraz udostępnienia wyników badań
- Dostęp zleceniodawcy do informacji dotyczących pobrania materiałów dla zleconych badań laboratoryjnych (tj. status realizacji zlecenia, dane pobrania: data, osoba pobierająca, nr próbki) z podsystemu Ruch chorych i Przychodnia.

6.2.2. System autoryzacji wyników badań laboratoryjnych z EDM w zakresie podpisu elektronicznego – 1 kpl.

L.p.	Charakterystyka (wymagania minimalne)
1	Rozwiązanie do autoryzacja wyników badań laboratoryjnych i możliwości odkładania ich do repozytorium EDM.
2	Wymiana dokumentacji medycznej pomiędzy LIS a HIS z dostępem do wyników badań przechowywanych w repozytorium EDM dla innych podmiotów medycznych jak i dla indywidualnych pacjentów.
3	System klasy LIS zintegrowany z HIS z wdrożonymi usługami umożliwiającymi podpis elektroniczny tworzonej dokumentacji medycznej umożlwiający powstanie EDM.

6.2.3. Modernizacja, wdrożenie e-Usług i integracja z RCIM

Projekt zakłada modernizację następujących istniejących e-usług:

- e-Informacja – modernizacja i rozszerzenie e-usługi w integracji z P1
- e-Rejestracja – modernizacja i rozszerzenie e-usługi w zakresie integracji z IKP na platformie P1

Projekt zakłada realizację następujących nowych e-usług:

- RREDM – Regionalne Repozytorium EDM

Projekt zakłada utrzymanie następujących istniejących e-usług:

- ERP – Elektroniczny Rekord Pacjenta
- EPW-ZOZ – Elektroniczna Platforma Współpracy ZOZ

Projekt zakłada rezygnację z dalszego utrzymania następujących istniejących e-usług:

- RRDR – Regionalny Rejestr Danych Ratunkowych

Warunkiem koniecznym w realizacji projektu jest zintegrowanie się z systemem PSIM. W zakresie integracji tworzonego systemu informatycznego placówki medycznej z warstwą regionalna PSIM, Wykonawca zobowiązany jest do wytworzenia interfejsów (za pomocą mechanizmów Web Services łączących system informatyczny SSI z RCIM). W ramach integracji przewiduje się realizację następujących zadań:

- Uruchomienie bezpiecznego kanału VPN konfiguracją i testowaniem kanału VPN niezbędnego do integracji na dostarczonym urządzeniu UTM.
- Przystosowanie oprogramowania lokalnego do wymiany informacji z komponentami PSIM w obszarze:
  - RREDM – Regionalne Repozytorium EDM – udostępnianie dodatkowych e-dokumentów na platformę regionalną wytworzonych w systemie HIS
  - e-Informacja – modernizacja i rozszerzenie e-usługi w integracji z P1E-usługa: EPN-Elektroniczna Platforma Nadzoru
  - e-Rejestracja – modernizacja i rozszerzenie e-usługi w zakresie integracji z IKP na platformie P1

Integracja ma być zgodna z wytyczani do konkursu projektu Podniesienie efektywności i dostępności e-usług Nr naboru RPPK.02.01.00-IZ.00-18-004/20. Informacja o naborze:
https://www.rpo.podkarpackie.pl/index.php/nabory-wnioskow/2426-2-1-podniesienie-efektywnosci-i-dostepnosci-e-uslug-nr-naboru-rppk-02-01-00-iz-00-18-004-20

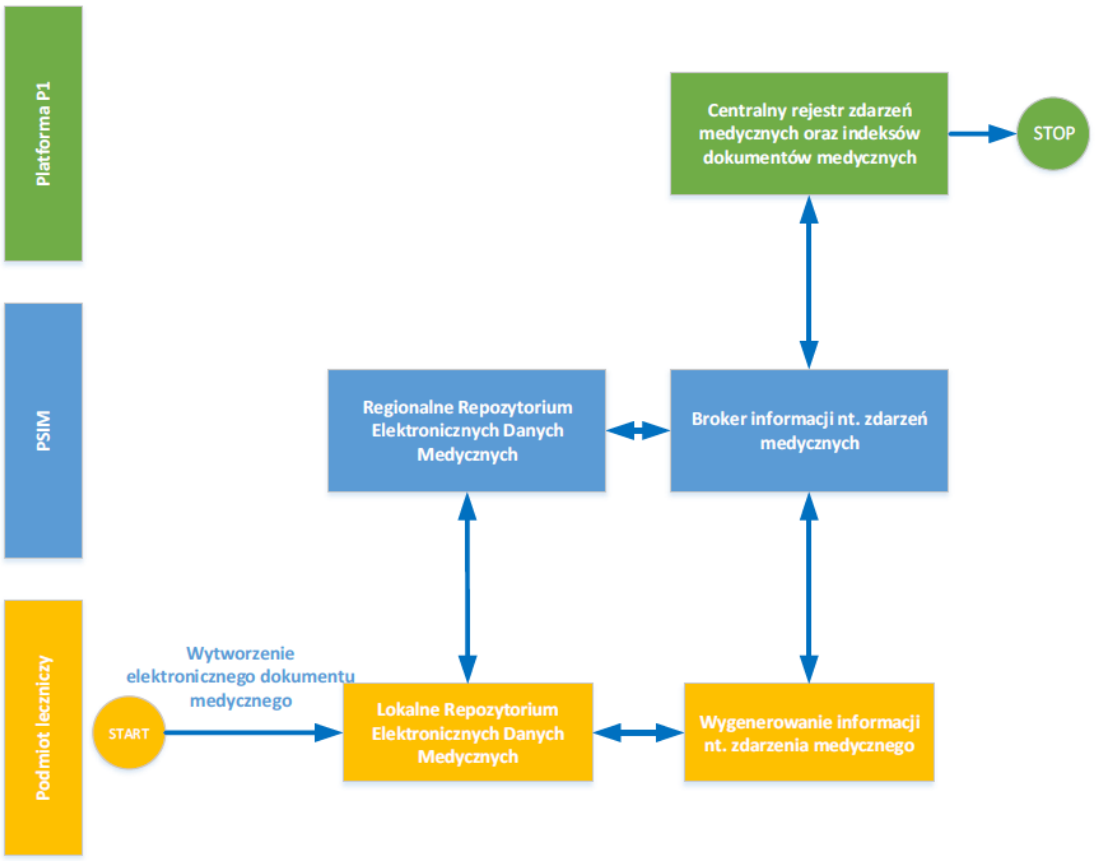
6.2.3.1. Dokumentacja projektowa

Dokument opisujący istniejącą (obecną) w placówce medycznej integrację wynikającą z realizacji wcześniejszego projektu PSIM:
https://www.rpo.podkarpackie.pl/images/dok/OS_II_VI/2019/nab_2_1_004/RK_11_2_Techniczne_warunki_integracji_z_RCIM_2_1_004_20.zip

Dokument opisujący docelowy model e-usług wymagający integracji (Rk_11_3 skrócony opis e-usług realizowanych w ramach modernizacji projektu - Podkarpacki system informacji medycznej – psim oraz karta integracji z RCIM po modernizacji usług):
https://www.rpo.podkarpackie.pl/images/dok/OS_II_VI/2019/nab_2_1_004/zm/RK_11_3_Skrocony_opis_e-uslug_w_ramach_modernizacji_PSIM_oraz_karta_integracji_z_RCIM_po_modernizacji.pdf

6.2.3.2. RREDM – Regionalne Repozytorium EDM -udostępnianie dodatkowych e-dokumentów na platformę regionalną wytworzonych w systemie HIS

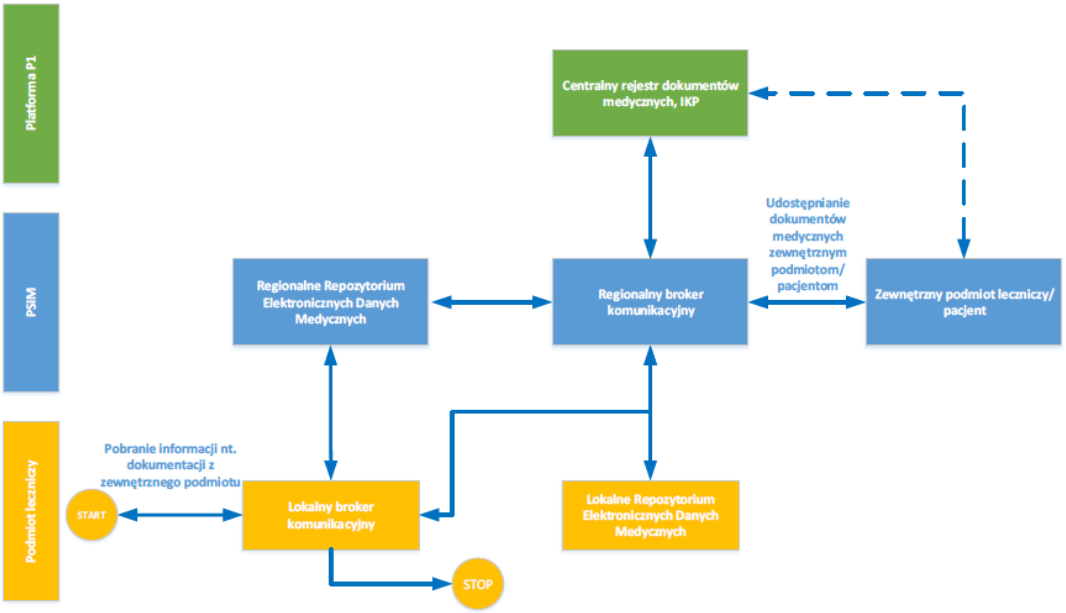
Opis stanu docelowego po modernizacji:



Rys. Schemat obrazujący przebieg procesu składowanie elektronicznych dokumentów medycznych pacjentów w ramach regionalnego repozytorium oraz wysyłania informacji do platformy P1 o zdarzeniach medycznych wygenerowanych w podmiotach leczniczych.

Usługa będzie pozwalała na składowanie w RREDM kopii elektronicznych dokumentów medycznych (format HL7 CDA) oraz elektronicznych danych obrazowych, będących wynikiem badań obrazowych, pacjentów (format DICOM) przekazanych z Lokalnego Repozytorium Danych Medycznych (LREDM). Poszczególne podmioty lecznicze będą miały dostęp do indywidualnych wskazanych zasobów/zbiorów zlokalizowanych w centrum regionalnym PSIM.
Umożliwienie składowania elektronicznych danych pozwoli też podmiotom leczniczym na wykorzystanie RREDM w roli długoterminowego archiwum, co z kolei przyczyni się do zmniejszenia

wymogów sprzętowych, w podmiotach, związanych z zapewnieniem archiwum dokumentacji elektronicznej.
Przekazywane przez podmioty dokumenty będą klasyfikowane ze względu na wymagany okres przechowywania, pozwoli to na wprowadzenie mechanizmów po stronie e-usługi kontrolujących terminowości przechowywania i niszczenia (usuwania) przeterminowanej dokumentacji medycznej pacjentów.



Rys. Schemat obrazujący przebieg procesu wymiany elektronicznych dokumentów medycznych pacjentów w ramach regionalnego repozytorium oraz z zewnętrznymi podmiotami leczniczymi/pacjentami z uwzględnieniem komunikacji z platformą P1.

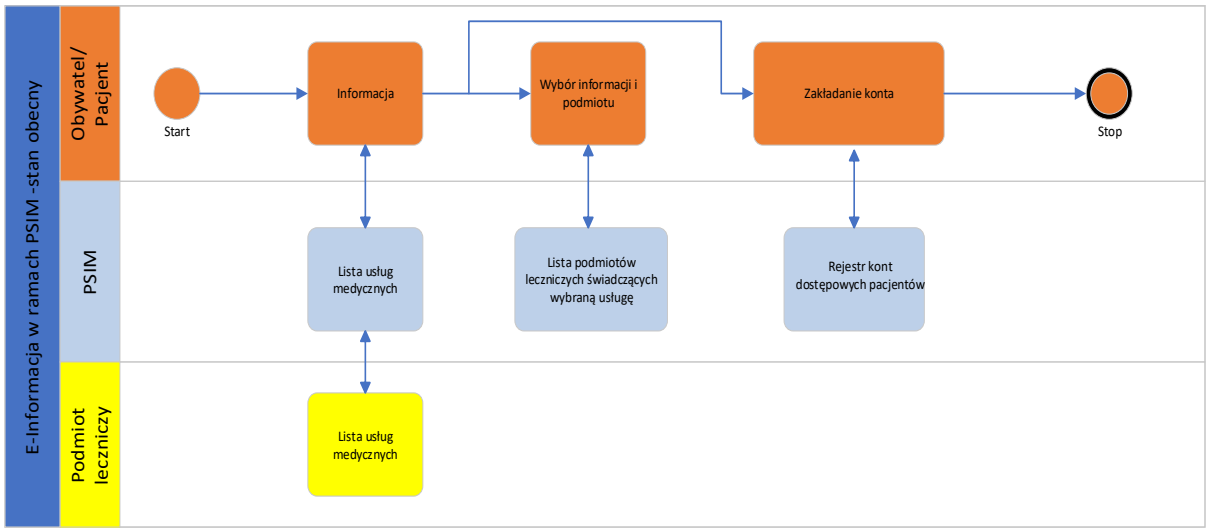
E-usługa będzie także pełniła rolę brokera w zakresie przekazywania informacji o zdarzeniach medycznych i indeksach elektronicznej dokumentacji medycznej, pomiędzy pomiotami leczniczymi zintegrowanymi z PSIM, a platformą P1.
Dodatkowo e-Usługa będzie pełniła rolę węzła pośredniczącego w wymianie elektronicznej dokumentacji medycznej pacjentów pomiędzy podmiotami leczniczymi zintegrowanymi z platformą PSIM oraz z zewnętrznymi podmiotami leczniczymi (także innymi platformami regionalnymi) z uwzględnieniem uprawnień do dostępu do dokumentacji medycznej nadanej przez pacjenta w IKP (Internetowym Koncie Pacjenta). Proces pobierania dokumentacji medycznej przez podmiot zintegrowany z PSIM zaczyna się od wyszukania indeksów dokumentów medycznych w rejestrze centralnym P1 wskazanego pacjenta i po autoryzacji oraz weryfikacji uprawnień do dokumentów po stronie P1 umożliwia pobrać wskazany dokument bezpośrednio ze zewnętrznego podmiotu leczniczego (zewnętrznego szpitalnego systemu informatycznego). Powyższy diagram przedstawia również proces obsługi wymiany dokumentów zgodny z ERP.

6.2.3.3. e-Informacja – modernizacja i rozszerzenie e-usługi w integracji z P1

Opis stanu obecnego

Funkcjonalności e-Informacji umożliwiają:

- Dostęp do informacji dotyczących opieki zdrowotnej
- Korzystanie z Informatora o usługach medycznych
- Wyszukiwanie usług medycznych realizowanych przez jednostki opieki zdrowotnej w regionie Podkarpacia
- Zakładanie i obsługę konta użytkownika końcowego, a także korzystanie z funkcjonalności dostępnych dla zalogowanych użytkowników
- Integrację danych



Rys. Opis stanu obecnego.

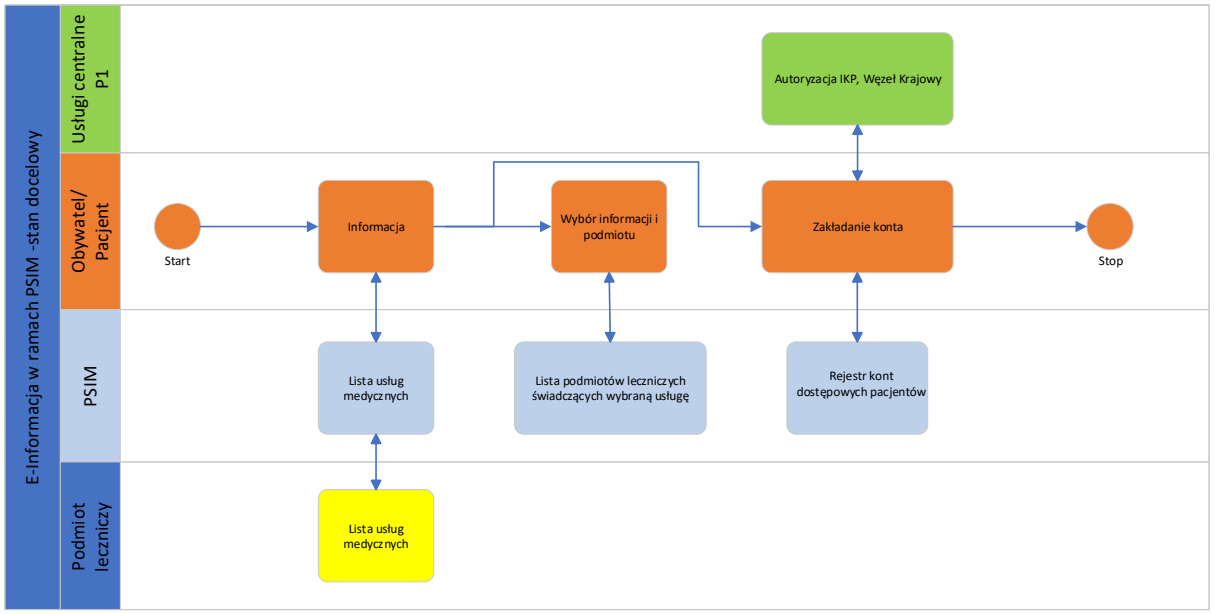
e-Usługa E-Informacja jest oprogramowaniem aplikacyjnym (portalem www) zlokalizowanym w warstwie regionalnej PSIM. Dostęp do funkcjonalności publikującej informacje dotyczące opieki zdrowotnej oraz usług medycznych realizowanych przez zintegrowane z RCIM jednostki opieki zdrowotnej jest możliwy poprzez przeglądarkę internetową i nie wymaga logowania.
W przypadku korzystania z treści, takich jak informacje ogólne dla pacjenta, Aktualności, Karta Praw Pacjenta, informacje o regulacjach prawnych pochodzące z dedykowanych serwisów informacyjnych lub katalog plików do pobrania użytkownik wybiera odpowiednią opcję z udostępnionych w ramach portalu www e-Informacja.
Informacje o usługach medycznych, dostępnych w jednostkach ochrony zdrowia zintegrowanych w ramach PSIM, są prezentowane z zasobów RCIM. W warstwie regionalnej gromadzone są dane o jednostkach ochrony zdrowia, ich strukturze organizacyjnej, usługach realizowanych przez poszczególne jednostki, o personelu realizującym usługi w danej jednostce ochrony zdrowia oraz o pierwszym wolnym terminie, na który można wykonać rejestrację na daną usługę. Wymienione informacje są zebrane w postaci katalogów:

- Katalog Jednostek Ochrony Zdrowia
- Katalog Usług
- Katalog Personelu
- Katalog Grafików

Podczas przeglądania danych o usługach medycznych przy każdej z usług występuje opcja umożliwiająca, poprzez jedno kliknięcie, przejście do usługi e-Rejestracja i rezerwację terminu wizyty.
Użytkownik ma możliwość wyszukiwania usług medycznych w prowadzonych w warstwie regionalnej Katalogach danych. Warstwa regionalna PSIM, po wyszukaniu danych spełniających określone kryteria w odpowiednich katalogach, prezentuje je użytkownikowi. Dla każdej z wyszukanych usług

medycznych dostępna jest informacja o orientacyjnym pierwszym wolnym terminie Rejestracji według danych zgromadzonych w Katalogu Grafików.
Każda wyświetlona w wynikach wyszukiwania usługa medyczna posiada opcję umożliwiającą przejście do usługi e-Rejestracja i rezerwację terminu wizyty.
W ramach funkcjonalności usługi istnieje możliwość założenia konta użytkownika końcowego w systemie PSIM. Zalogowanym użytkownikom końcowym dostarczane są dodatkowe funkcjonalności. Są to m.in.: obsługa otrzymywanych i wysyłanych wiadomości systemowych, rejestrowanie i obsługa subkont przez opiekunów (np. rodzica dziecka, przedstawiciela ustawowego), konfiguracja własnego konta (np. dane kontaktowe), a także dostęp i wizualizacja dla funkcjonalności innych e-Usług (np. e-Rejestracja, przeglądanie i wprowadzanie dodatkowych danych ratunkowych).
Funkcjonalność zakładania konta użytkownika końcowego i logowania się jest dostępna na portalu www i jej użycie nie wymaga logowania. Funkcjonalności dotyczące obsługi konta wymagają autoryzacji.
Regionalne katalogi danych w RCIM są zasilane danymi z lokalnych systemów medycznych HIS w zakresie wymaganym do prezentacji aktualnej informacji w ramach usługi e-Informacja. Zasilenie odbywa się za pomocą udostępnianych interfejsów o zdefiniowanej strukturze. Zasilanie rozpoczyna się w momencie automatycznego uruchomienia procesu ładowania, wynikającego z częstotliwości zasilania zdefiniowanej w Module Administracji Regionalnej. Warstwa regionalna przekazuje żądanie synchronizacji danych do poszczególnych jednostek ochrony zdrowia. W każdej z jednostek system lokalny udostępnia przygotowane dane portalowe. RCIM weryfikuje poprawność danych i dokonuje zapisu w odpowiednich katalogach.

Opis stanu docelowego po modernizacji



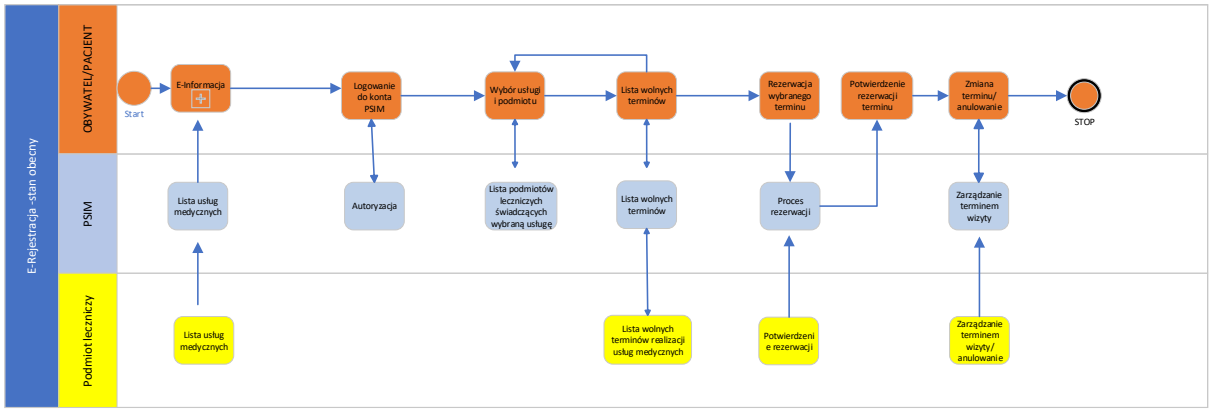
Rys. Schemat obrazujący przebieg docelowego procesu informowania o usługach oraz zakładania konta przez pacjenta.

Pacjent po wejściu na zmodernizowany portal WWW PSIM będzie miał możliwość otrzymania informacji nt. zakresu usług, struktury organizacyjnej poszczególnych podmiotów podłączonych do platformy regionalnej. Dane te będą pobierane z rejestrów znajdujących się w systemach lokalnych. Zasilenie danymi z lokalnych systemów informatycznych podmiotów leczniczych odbywać się będzie w sposób automatyczny na podstawie aktualnych danych zgromadzonych w lokalnych systemach informatycznych podmiotów medycznych podłączonych do PSIM bez konieczności udziału osób trzecich.

Pacjent ma możliwość założenia konta dostępowego w platformie regionalnej, natomiast konto do momentu aktywacji poprzez osobistą wizytę we wskazanym podmiocie leczniczym lub poprzez profil zaufany jest nieaktywne.
E-usługa po modernizacji będzie usługą publiczną i będzie rozszerzała zakres obecnej e-usługi e-Informacja o możliwość uwierzytelniania użytkowników korzystających z e-usług na platformie regionalnej o mechanizm uwierzytelnienia za pośrednictwem węzła krajowego (WK) oraz pozwoli na szersze wykorzystanie informacji o podmiotach leczniczych zintegrowanych z PSIM w zakresie struktury organizacyjnej, personelu świadczącego usługi i usług zdrowotnych realizowanych przez te podmioty. W ramach tej e-usługi pacjentom udostępniony zostanie m.in. Informator o usługach medycznych oraz Wyszukiwarka usług medycznych opierająca się na danych pozyskiwanych z lokalnych systemów informatycznych w podmiotach leczniczych.

6.2.3.4. e-Rejestracja – modernizacja i rozszerzenie e-usługi w zakresie integracji z IKP na platformie P1

Opis stanu obecnego



Rys. Opis stanu obecnego usługi e-Rejestracja.

Funkcjonalności e-Rejestracji umożliwiają:
- Rezerwację usług medycznych w jednostkach ochrony zdrowia zintegrowanych z RCIM za pośrednictwem portalu internetowego przez zarejestrowanych na poziomie regionalnym użytkowników końcowych (pacjentów),
- Anulowanie wskazanej na liście rejestracji,
- Śledzenie zdarzeń związanych z rejestracją za pomocą systemu komunikatów (powiadomień) dla użytkowników końcowych, w formie wiadomości e-mail i SMS, dotyczących: potwierdzenia rejestracji, zbliżającego się terminu wizyty, anulowania wizyty oraz zmiany terminu wizyty.

Użytkownik ma możliwość rezerwacji terminu wizyty na wybraną usługę medyczną, wykonywaną przez jednostkę ochrony zdrowia, za pomocą usługi internetowej udostępnianej na portalu e-Informacja lub na lokalnym portalu internetowym jednostki ochrony zdrowia.
Z e-Rejestracji mogą korzystać wyłącznie zarejestrowani na poziomie regionalnym użytkownicy końcowi. W celu wykonania rejestracji użytkownik musi być zalogowany do konta użytkownika końcowego umiejscowionego w warstwie regionalnej RCIM. Logowanie odbywa się za pomocą jednej z funkcjonalności usługi e-Informacja.
Użytkownik rozpoczyna rezerwację terminu wizyty od wyszukania i wybrania odpowiedniej usługi medycznej realizowanej we wskazanej jednostce ochrony zdrowia. Odbywa się to w ramach funkcjonalności usługi e-Informator. Użytkownik wskazuje wolny termin, z dokładnością do dnia

i godziny, oraz – w zależności od usługi i jednostki ochrony zdrowia – konkretny personel lub konkretne miejsce wykonania usługi. W warstwie RCIM następuje walidacja kolizji rezerwacji polegająca na sprawdzeniu, czy istnieją wielokrotne rezerwacje różnych usług jednego dnia na tę samą godzinę, co wskazany termin. Następnie warstwa regionalna PSIM przekazuje do odpowiedniej jednostki ochrony zdrowia żądanie zablokowania wskazanego terminu wizyty w systemie medycznym. System lokalny blokuje wskazany termin jest na określony czas. Termin wizyty jest odblokowywany w przypadku przerwania sesji lub braku potwierdzenia przez użytkownika rezerwowanej wizyty na zakończenie dokonywania rezerwacji. Następnie użytkownik wprowadza dane wymagane do rejestracji na wyświetlonym przez system regionalny formularzu rejestracji i zatwierdza je. Przed przekazaniem danych do warstwy lokalnej system regionalny weryfikuje poprawność wypełnienia formatki rejestracji i kompletność wymaganych danych. Jeżeli dane są poprawne, to system regionalny wysyła je do odpowiedniej jednostki ochrony zdrowia w celu zarejestrowania pacjenta. Jeżeli nie można wykonać rejestracji, to system lokalny przekazuje do RCIM informację o jej odrzuceniu i zwalnia wstępną rezerwację wybranego terminu, a warstwa regionalna informuje użytkownika o odrzuceniu rezerwacji terminu wizyty. Jeżeli pacjent może zostać zarejestrowany, to system lokalny w terminie wstępnej rezerwacji zapisuje rejestrację pacjenta i przekazuje do RCIM potwierdzenie przyjęcia rejestracji. Warstwa regionalna informuje użytkownika o przyjęciu rezerwacji terminu wizyty wyświetlając odpowiedni komunikat na ekranie, zapisuje rejestrację w danych przechowywanych na koncie użytkownika oraz wysyła do użytkownika końcowego powiadomienia potwierdzające rejestrację.

Użytkownik końcowy może zrezygnować z terminu zaplanowanej wizyty, czyli anulować rejestrację w lokalnym systemie medycznym. Anulowanie wizyty jest możliwe z poziomu e-usługi e-Informacja.

W celu anulowania rejestracji użytkownik musi być zalogowany do swojego konta. Anulowanie terminu wizyty odbywa się poprzez wskazanie wybranej rezerwacji i wybranie odpowiedniej opcji. W efekcie system lokalny anuluje wskazaną rejestrację i przekazuje do warstwy regionalnej potwierdzenie anulowania, system regionalny zmienia status rejestracji w RCIM i zapisuje odpowiedni status na koncie użytkownika oraz powiadamia go o anulowaniu terminu wizyty.

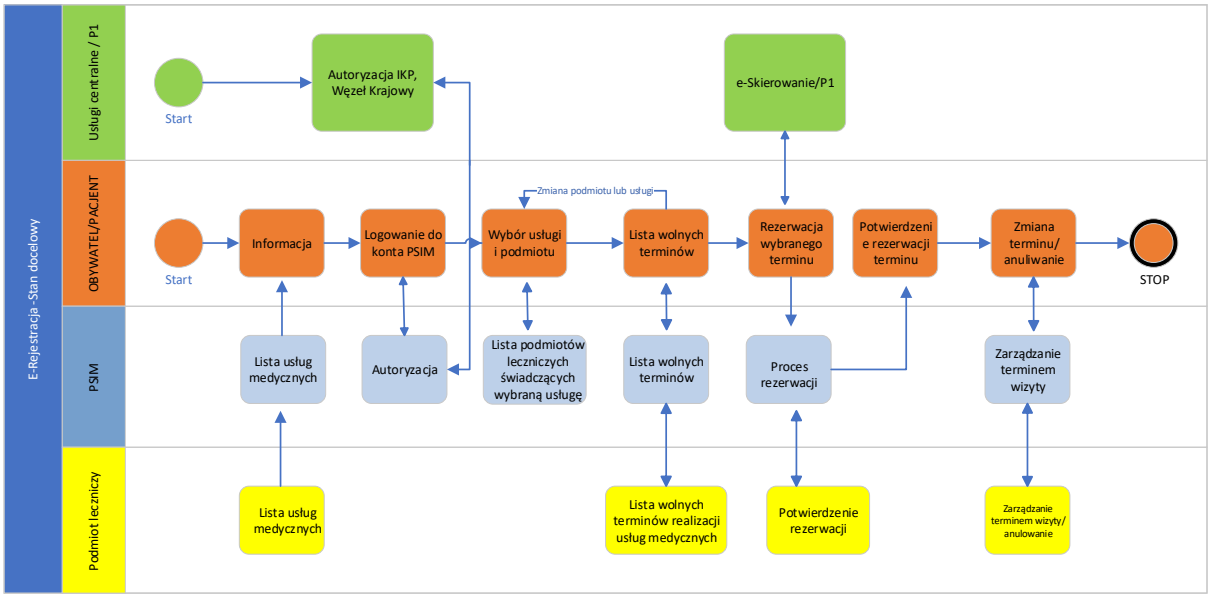
W ramach usługi e-Rejestracja funkcjonuje system komunikatów (powiadomień dla użytkowników końcowych w formie wiadomości e-mail i SMS) dotyczących:

- potwierdzenia rejestracji,
- zbliżającego się terminu wizyty,
- anulowania wizyty,
- zmiany terminu wizyty (zarówno przez użytkownika jak i w lokalnym systemie medycznym HIS).

Komunikaty systemowe SMS i e-mail są obsługiwane dla wszystkich sposobów rejestracji (poprzez WWW, telefon, osobiście) dla użytkowników posiadających konto Użytkownika Końcowego. Zawartość komunikatu z powiadomieniem o zdarzeniu jest przekazywana do warstwy regionalnej przez lokalny system medyczny. Sposób powiadamiania – wysyłanie wiadomości e-mail lub wiadomości SMS lub wysyłanie obydwu rodzajów wiadomości – zależy od konfiguracji wykonanej w Module Administracji Regionalnej oraz parametryzacji konta użytkownika końcowego.

Po otrzymaniu przez warstwę regionalną informacji o zakończeniu wizyty w lokalnym systemie medycznym system regionalny zmienia status rejestracji w RCIM w danych gromadzonych na koncie użytkownika końcowego.

Opis stanu docelowego po modernizacji



Rys. Schemat obrazujący docelowy przebieg procesu rejestracji pacjenta na wybraną usługę medyczną.

W ramach procesu obsługi pacjenta planowane jest dostarczenie zmodyfikowanych e-usług publicznych : e-Informacja oraz e-Rejestracja.
Istotą nowych e-usług, a tym samym zmianą procesu obsługi pacjenta jest dostarczenie aktualnych i rzeczywistych danych nt. podmiotów leczniczych zintegrowanych z PSIM w zakresie struktury organizacyjnej, dostępnego personelu medycznego oraz zakresu usług i procedur medycznych realizowanych w danym podmiocie.
Dodatkowo rozbudowana integracja z systemami informatycznymi w podmiotach leczniczych pozwoli na dostęp do listy wolnych terminów wizyt wraz z możliwością automatycznej rezerwacji przez pacjenta wybranego terminu (docelowo z wykorzystaniem e-Skierowania). Obsługa procesu rezerwacji będzie w pełni zautomatyzowana (wykorzystanie standardu HL7 FHIR), co wyklucza konieczność udziału w tym procesie personelu rejestracyjnego podmiotów leczniczych, a pacjent w momencie rezerwacji terminu poprzez PSIM rezerwuje go w terminarzu w systemie informatycznych podmiotu leczniczego.
Zmianie też ulegnie proces zakładania konta dostępowego w PSIM przez pacjenta. Pacjent chcący skorzystać z funkcjonalności wymagających uwierzytelnienia na platformie PSIM, będzie przekierowywany na dedykowaną stronę w ramach IKP, zawierającą informacje dla użytkowników portali regionalnych oraz link do strony logowania z użyciem Węzła Krajowego (WK). Po uwierzytelnieniu w IKP za pośrednictwem WK, użytkownik będzie przekierowywany z powrotem na stronę PSIM. Dla pacjentów którzy posiadają konta dostępowe w PSIM nadal będzie możliwe zalogowanie z wykorzystaniem dotychczasowych danych natomiast po zalogowaniu pacjent będzie musiał przejść proces autoryzacji w IKP/węźle krajowym.

Z poziomu platformy pacjentem będzie mógł zarządzać swoim terminarzem wizyt w szczególności będzie mógł je anulować, dodatkowo wizyty umówione bezpośrednio w placówkach/telefonicznej także będą dostępne w terminarzu pacjenta umówionych wizyt w platformie PSIM.
Jest to publiczna elektroniczna usługa umożliwiająca rejestrację pacjentów na wizyty w jednostkach opieki zdrowotnej (zintegrowanych z PSIM). Elektroniczna rejestracja odbywa się z wykorzystaniem portalu WWW i/lub interfejsów umożliwiających współpracę systemów lokalnych jednostek opieki zdrowotnej z platformą. Usługa jest dedykowana obywatelom oraz jednostkom opieki zdrowotnej.
E-usługa umożliwia pacjentom rezerwację terminów wizyt przez Internet bez angażowania personelu medycznego przychodni. Jest dostępna 24 godziny na dobę, przez 7 dni w tygodniu. Pacjent nie musi osobiście pojawić się w okienku rejestracji, nie musi także dzwonić do podmiotu leczniczego. Wystarczy, że wejdzie na stronę internetową PSIM, a grafik rejestracji internetowej umożliwi samodzielny i łatwy wybór lekarza oraz dostępnych terminów wizyt.
Funkcjonalności e-Rejestracji umożliwiają:

- Rezerwację usług medycznych w jednostkach ochrony zdrowia zintegrowanych z PSIM za pośrednictwem portalu internetowego przez zarejestrowanych na poziomie regionalnym użytkowników końcowych (pacjentów),
- Anulowanie wskazanej na liście rejestracji,
- Śledzenie zdarzeń związanych z rejestracją za pomocą systemu komunikatów (powiadomień) dla użytkowników końcowych, w formie wiadomości e-mail i SMS, dotyczących: potwierdzenia rejestracji, zbliżającego się terminu wizyty, anulowania wizyty oraz zmiany terminu wizyty.

Ze zmodernizowanej e-Rejestracji mogą korzystać wyłącznie uwierzytelnieni za pośrednictwem węzła krajowego (WK) pacjenci i posiadający konto pacjenta w PSIM. Proces logowania będzie się odbywał z wykorzystaniem zmodernizowanej usługi e-Informacja.

6.2.3.5. Wdrożenie e-Usług i integracja z RCIM

W projekcje Zamawiający wymaga od Wykonawcy integracji z e-usługami na poziomie Regionalnym PSIM/RCIM. Wykonawca musi zapewnić przekazywanie danych do systemów regionalnych z lokalnego systemu poprzez instalację i konfigurację lokalnych interfejsów integracji i wymiany danych.

Zamawiający w ramach integracji oczekuje takiej sytuacji, w której po zakończeniu projektu będzie w stanie realizować e-usługi wskazane w niniejszym dokumencie na platformie regionalnej PSIM.
Uruchomienie zmodernizowanych e-usług będzie miało miejsce w momencie, gdy integracja ze zmodernizowaną warstwą regionalną będzie możliwa.

W ramach integracji Wykonawca zobowiązany będzie do dostarczenia odpowiednich mechanizmów integrujących (szyna danych / broker) pozwalających na wymianę danych pomiędzy zmodernizowanym oprogramowaniem dziedzinowym, dostarczonymi modułami oraz systemem regionalnym RCIM.
Szyna danych ma zapewnić komunikację pomiędzy komponentami projektu na poziomie lokalnym, nie jest elementem systemu regionalnego RCIM/PSIM.

Szyna danych musi zapewniać:

- Podłączanie, katalogowanie i wzajemne udostępnianie usług pomiędzy systemami dziedzinowymi oraz pozostałymi elementami, modułami implementacji programowej,
- Wspomaganie definiowania implementacji, wdrażanie i zarządzanie usługami realizującymi dostęp do integrowanych systemów,
- Posiadanie mechanizmu umożliwiającego planowe i cykliczne uruchamianie usług platformy,

- Zarządzanie planowanymi do uruchomienia usługami tak aby odbywało się to w sposób spójny z jednego miejsca platformy na zasadzie definiowania harmonogramu wywołań,
- Musi wspierać co najmniej następujące standardy komunikacji: SOAP, JMS, HTTP, HTTPS, FTP, SFTP, SMTP, SMTPS, POP3, POP3S, IMAP oraz obsługiwać translację komunikatów pomiędzy tymi protokołami,
- Obsługę protokołu SOAP i Web Services dla usług konsumowanych jak i udostępnianych,
- możliwość konsumowania oraz udostępniania usług w standardzie webservices (WSDL 1.1, SOAP 1.2, SOAP with Attachments),
- Zgodność ze standardem WS-Addressing,
- Zgodność ze standardem WS-Security,
- Zgodność ze standardem WS-AtomicTransaction,
- Zgodność ze standardem WS-Policy,
- Wykorzystanie rejestrów UDDI (UDDI 3.0).

Wdrożone e-Usługi i powiązane z nimi oprogramowanie komunikacyjne i mechanizmy integracyjne z RCIM (np. szyna danych / broker) powinno posiadać min. 48-miesięczną gwarancję liczoną od dnia podpisania protokołu odbioru (w skład której wchodzi zapewnienie poprawności działania, prawo do aktualizacji).